普通高等教育"十一五"国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会
共同指导

顾问委员会主任：沈昌祥　编委会主任：肖国镇

VPN虚拟专用网安全实践教程

金汉均　仲　红　汪双顶　编著

http://www.tup.com.cn

Information Security



清华大学出版社

高等院校信息安全专业系列教材

VPN虚拟专用网安全实践教程

金汉均　仲　红　汪双顶　编著

清华大学出版社
北　京

内 容 简 介

本书主要介绍使用 VPN 技术组建安全网络实践教程，全书分为两个知识模块，分别为组建虚拟专用网安全基础知识，和使用虚拟专用网安全产品组建虚拟专用网实践教程。知识点包括：构建站点到站点 IPSec，站点到站点 IPSec VPN（数字签名），IPSec VPN，远程访问 IPSec VPN（用户口令），远程访问 IPSec VPN（USB-Key 数字证书），远程访问 IPSec VPN 的授权控制，使用桥接模式构建 IPSec VPN，使用路由器构建 GRE VPN，使用路由器构建 GRE over IPSec VPN，在地址重叠环境中部署 IPSec VPN，远程访问 IPSec VPN 准入控制，构建 SSL VPN，构建 SSL VPN 单臂通信实验等。全书在每个章节中，对所使用到相关安全产品的基本配置、基本界面、功能配置，都进行详细的讲解，以帮助读者熟悉产品的使用，并进一步诠释了其在工程项目中的实施方法。

本书可作为高等院校计算机科学与技术、通信工程、计算机网络等相关专业本科生或研究生，学习和研究网络安全产品及技术的实验教材。此外本书还可作为网络安全专业认证的培训教材以及网络设计师、网络工程师、系统集成工程师以及其他专业技术人员技术参考书。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目（CIP）数据

VPN 虚拟专用网安全实践教程 / 金汉均等编著．—北京：清华大学出版社，2010.1
（高等院校信息安全专业系列教材）
ISBN 978-7-302-21234-8

Ⅰ．V…　Ⅱ．金…　Ⅲ．虚拟网络－高等学校－教材　Ⅳ．TP393.01

中国版本图书馆 CIP 数据核字(2009)第 174742 号

责任编辑：谢　琛　李玮琪
责任校对：焦丽丽
责任印制：

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185×260　　**印　张**：14.5　　**字　数**：341 千字
版　　次：2010 年 1 月第 1 版　　**印　　次**：2010 年 1 月第 1 次印刷
印　　数：1～0000
定　　价：0.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：-

创新网络教材编辑委员会

（院校成员名单排名不分先后）

王继龙	男	清华大学网络中心
王晓东	男	宁波大学计算机科学学院
王昭顺	男	北京科技大学计算机系
王　玲	女	四川师范大学信息技术学院
刘　琪	女	中南财经政法大学信息技术学院
汪　涛	男	解放军炮兵学院指挥自动化与仿真系
邵　丹	女	长春大学计算机学院
余明辉	男	番禺职业技术学院软件学院
闵　林	男	河南大学网络中心
陈红松	男	北京科技大学计算机系
孟晓景	男	山东科技大学信息科学与工程学院
张国清	男	辽宁交通高等专科学校信息工程系
林　楠	女	郑州大学软件技术学院
武俊生	男	山西大学工程学院信息系
杨　璐	女	中国农业大学计算机系
杨　威	男	山西师范大学网络信息中心
金汉均	男	华中师范大学计算机科学系
姚　羽	男	东北大学信息科学与工程学院
贺　平	男	番禺职业技术学院软件学院
俞黎阳	男	华东师范大学计算机科学技术系
黄传河	男	武汉大学计算机学院
鲍　蓉	女	徐州工程学院电信工程学院
裴纯礼	男	北京师范大学教育技术学院

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点如下：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教

材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

"高等院校信息安全专业系列教材"已于2006年初正式列入普通高等教育"十一五"国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育"十一五"国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。"高等院校信息安全专业系列教材"将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断修订和完善。

我们的E-mail地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

清华大学出版社

前 言

21世纪，随着人类步入信息社会，信息产业正成为全球经济发展的主导产业。计算机科学与技术在信息产业中占据了重要的地位，随着互联网技术的普及和推广，网络技术更是信息社会发展的推动力，人们日常学习、生活和工作都越来越依赖于网络，因此信息技术、信息安全技术和网络安全技术正发展成为越来越重要的学科。

互联网技术的发展改变了人们的生活，今天信息安全内涵已发生了根本变化。安全已从一般性的安全防卫，变成了一种非常普通的安全防范；从一种研究型的安全学科，变成了无处不在，与人们学习、生活和工作息息相关的安全技术。技术的普及也推动了社会对人才的需求，因此建立起一套完整的网络安全课程教学体系，提供体系化的安全专业人才培养计划，培养一批精通安全技术的专业人才队伍，对目前高校计算机网络安全方向专业人才的培养，显得尤为重要。

1. 关于教材开发背景

结合国家"十一五"本科计算机专业课程规划体系，以及深入领会教育部计算机科学与技术教学指导委员会编制的"计算机科学与技术专业规范的知识体系和课程大纲"文件精神，为及时反映目前网络安全专业学科发展动态，创新网络教材编辑委员会组织编写了本书。希望编撰的网络安全知识，既重视理论、方法和标准的介绍，又兼顾技术、系统和应用分析，在内容结构和知识点布局上还有所创新。

此外随着互联网技术的普及和推广，日常学习和工作依赖于网络的比重增加，计算机网络安全的实施和防范技术，成为目前最为瞩目的学习内容。根据上述思路，创新网络教材编辑委员会选择网络安全技术在生活中具体应用，作为教材开发主线，规划出面向实际工程案例，可操作、可应用、可实施的网络安全技术教程。更希望规划的安全技术直观、形象、具体、可落实，选编和规划的安全知识具有专业化、体系化、全面化特征，能体现和代表当前最新的网络安全技术发展方向。

2 关于教材指导思想

通过市场调查发现，指导计算机网络安全实践教学内容的教材非常缺乏。翻阅市场上数量有限的安全类教材，这些教材品种都偏重于网络安全理论诠释，而针对实际网络安全工程实施、可在课堂中动手实施的甚少。正是

基于此，创新网络教材编辑委员会组织国内院校一线教师，联合来自厂商专业工程师，联合开发了这本覆盖网络安全技术专业教程，希望培养学生对网络安全技术动手能力。

和同类以网络安全技术为研究方向的专业书籍相比，本书更注重实际工作中遇到的安全问题的解决能力。全书以安全技术应用为主线，以培养学生安全问题解决能力为目标，以加强实际安全技能锻炼为根本，满足学校安全类课程实践教学需要。因此全书在开发过程中，强化实践教学能力的培养，着重讲授生活中的网络安全问题，诠释对应的安全策略配置，最后依据学校提供的安全实践教学平台，直观、形象地诠释安全技术，帮助学生理解抽象的网络安全专业理论。

3. 关于教材开发内容

本书主要是针对高等院校计算机科学与技术、通信工程、计算机网络等相关专业，在计算机网络基础理论、网络安全基础理论学习完成之后，学习 VPN 技术的网络安全实践教程的配套用书。全书分为两个知识模块，分别介绍组建虚拟专用网安全基础知识和使用虚拟专用网安全产品组建虚拟专用网实践教程。知识点包括：构建站点到站点 IPSec，站点到站点 IPSec VPN（数字签名），IPSec VPN，远程访问 IPSec VPN（用户口令），远程访问 IPSec VPN（USB-Key 数字证书），远程访问 IPSec VPN 的授权控制，使用桥接模式构建 IPSec VPN，使用路由器构建 GRE VPN，使用路由器构建 GRE over IPSec VPN，在地址重叠环境中部署 IPSec VPN，远程访问 IPSec VPN 准入控制，构建 SSL VPN，构建 SSL VPN 单臂通信实验等。全书在每个章节中，对所使用到相关安全产品的基本配置，基本界面、功能配置，都进行详细的讲解，以帮助读者熟悉产品的使用，并进一步诠释其在工程项目中的实施方法。

全书包括近十几个难度不同的组建虚拟专用网络安全实验，适合学生循序渐进地学习，可作为高等院校计算机科学与技术、通信工程、计算机网络等相关专业本科生或者研究生，计算机网络工程、网络安全课程实验教材。全书实验设计，以工程项目需求为依据，旨在加深学生对组建虚拟专用网所涉及的安全工程理论知识的理解，提高学生组建虚拟专用网络实践能力、分析问题的能力和解决问题的能力。

4. 关于教材使用方法

全书提供的近十多个组建虚拟专用网络安全实验，帮助学生熟练掌握网络安全工程师所需要的基本技能。所有实验操作都以日常安全需求为主线串接知识，以问题解决过程作为核心，因此教师在使用本书时，可以作为相关安全理论学习完成之后的实验补充，帮助学生加强对抽象安全理论的直观理解。也可以根据教学的实际情况，从中选择部分组建 VPN 网络实验内容，要求学生在学完理论之后，通过适当数量和难度的实验来补充理论诠释的不足。由于书中全部内容都来自厂商实际工程案例，本书可作为就业前实习用书，通过一定数量组建虚拟专用网络安全工程案例学习，积累实际的组建虚拟专用网安全施工经验，以增强施工能力和故障排除能力。

5. 关于课程环境安排

本书覆盖计算机网络安全规划、组建和配置中涉及主流安全设备配置、管理技术，书中所有项目都来自于企业多年积累的工程案例。经过提炼，按照再现企业工程项目的组

织方式进行串接，每个工程项目都详细介绍了工程名称、工程背景、技术原理、工程设备、工程拓扑、工程规划、工作过程、结果验证等多个环节，循序渐进再现企业工程项目施工过程，并把这些工程在网络实验室中搭建出来，积累工作中的施工经验。

为顺利实施本教程，除需要对网络技术有学习的热情之外，还需要具备基本的计算机、网络、安全基础知识。这些基础知识为学习者提供一个良好的脚手架，帮助理解本书中的技术原理，为网络技术的进阶提供良好帮助。为做好这些安全实验，还需要为本课程提供一个可实施交换、路由、无线和安全实验的网络环境，再现企业网络工程项目。这种课程工作环境包括：一个可以容纳 40 人左右的网络实验室；不少于 4 组实验台。每组实验台中包括的组网实验设备有：二层交换机、三层交换机、模块化路由器、VPN 安全设备、网络防火墙、测试计算机和若干根网络连接线（或制作工具）。

虽然本书选择的组建虚拟专用网工程项目来自厂商案例，使用的组建虚拟专用网实验设备来自厂商，但本课程在规划中力求全部的关于虚拟专用网知识诠释和 VPN 技术选择都具有通用性，遵循行业内通用技术标准和行业规范。全书中关于设备的功能描述、接口标准、技术诠释、协议细节分析、命令语法解释、命令格式、操作规程、图标和拓扑图形的绘制方法，都使用行业内的标准，以加强其通用性。

6. 关于课程时间安排

本书希望加强学生组建虚拟专用网设备的实践操作，积累未来到一线组建安全 VPN 网络的工程施工经验，让学生深入地理解组建虚拟专用网中使用到相关安全设备的配置，熟悉组建虚拟专用网项目发生的场景，掌握施工过程。此外借助网络安全实验平台，还可以学习组建虚拟专用 VPN 网络安全设计、网络攻防和故障性能分析等相关知识，加强学生对网络安全技术的理解和掌握，培养学生的动手实践能力和设计分析能力，培养创新型人才。

本书可作为高等院校计算机科学与技术、通信工程、计算机网络等相关专业本科生或研究生，学习、研究网络安全技术的实验教材。其前导性的课程包括计算机网络、局域网组建、路由和交换技术等基础性网络技术。本书的课程安排时间在 36～72 学时不等，根据学校具体教学计划安排来确定，可选择全部的内容作为实验对象，也可选择部分内容作为实验对象。课程时间一般安排在三年级学期段，学生在学完基础网络技术后，作为基础技术的提高和补充。此外本书还可以作为社会上培训企业网络安全专业认证的培训教材以及网络设计师、网络工程师、系统集成工程师以及其他专业技术人员的技术参考书。

7. 关于课程资源

不同的专业课程教学都具有其本身的针对性。强化网络安全技术专业实践能力、强化安全技术应用和安全技能素养的培养，是本课程区别于传统网络安全专业课程特色之一。即使在目前众多以技能为教学实验课程中，本课程也具有其他课程不能比拟的特性。无论是前期为保证课程的有效实施，方便学校的管理，在课程实施环境（网络实验室）上投入资金，还是在课程规划上的创新、实验手段的多样性上，本课程在研发上投入的人力、物力都具有绝对优势。

为有效保证课程实验的有效实施，保证课程教学资源的长期提供，安全案例的积累、

最新安全技术的更新、新技术的学习、课程学习中的技术交流和讨论等，本课程的研发队伍为此还专门投入人力和物力，为本课程建设有专门的实践教学俱乐部资源共享基地，以有效支持课程在实施的过程中，资源的更新，疑难问题的解决，课程实施讨论等一系列支持和服务工作，详细内容可以访问和本课程配套网站：http://www.labclub.com.cn，在网站上可以获得更多的资源支持。

8. 关于课程开发队伍

本书由创新网络教材编辑委员会组织来自院系教学一线的专家、教师，联合来自厂商专业工程师协作编写完成。这些工作在各行业内的专家，把自己多年来在各自领域中积累的网络组建虚拟专用网安全技术及工作经验，以及对组建虚拟专用网络安全技术的深刻理解，凝结成本书。

金汉均博士，华中师范大学计算机科学系教授，主要研究方向是"网上虚拟现实中的关键技术和最优化算法应用"等。近年来，其在网络安全领域的研究也具有突出成就，发表了大量论文，其中十五篇被世界SCI，EI，ISTP三大检索企业收录。其长期在教学一线从事网络工程技术的教学经验和研究工作成果，以及其在网络安全领域的技术积累，为全书技术方向引导、知识体系的选择、技术的诠释方法正确性提供了重要保证。

仲红教授，2005年中国科学技术大学计算机系博士研究生毕业，获工学博士学位。硕士生导师。安徽省高校首批中青年骨干教师培养对象，现为网络安全专业建设带头人。

汪双顶高级工程工程师，毕业于北京师范大学，硕士。熟悉思科网络和锐捷网络产品及方案，拥有厂商的工作经历，以及面对不同厂商的安全设备，针对应用和实施网络安全防范的能力。他拥有多年在网络一线从事工程师、培训讲师的工作背景，参与过多个网络工程整网安全的规划、有实施经历，对再现企业安全工程实验的体例和样式起到结构形成作用。

此外在本书的编写过程中，还得到了其他一线教师、技术工程师等的大力支持。他们积累多年的来自教学和工程一线的工作经验，为本书的真实性、专业性、教学的方便性和实施的方便性提供了有力的支持。

本书规划、编辑的过程历经三年多的时间，前后经过多轮修订，得到很多人力支持，其改革力度之大，远远超过前期策划者原先的估计，加之课程组文字水平有限，错漏之处在所难免，敬请广大读者指正(labserv@ruijie.com.cn)！

创新网络教材编辑委员会

使用说明

为帮助学生全面理解安全技术细节，建立直观的网络安全印象，本书每一实验开始环节，都为读者引入一个来自企业真实网络安全问题，建立教学、学习环境，让读者深入到网络安全的环境中，了解本节安全知识内容，了解发生在真实网络工程项目中的场景，了解相应施工中需要的技术。

在全书关键技术解释和工程方案实施中，会涉及一些网络专业术语和词汇，为方便大家今后在工作中的应用，全书采用业界标准的技术和图形绘制方案。全书中使用相关的符号，以及网络拓扑图形惯有的风格和惯例，本书中使用的命令语法规范约定如下。

- 竖线“|”表示分隔符，用于分开可选择的选项。
- 星号“*”表示可以同时选择多个选项。
- 方括号“[]”表示可选项。
- 大括号“{}”表示必选项。
- 粗体字表示按照显示的文字输入的命令和关键字。在配置的示例和输出中，粗体字表示需要用户手工输入的命令（例如 **show** 命令）。
- 斜体字表示需要用户输入的具体值。

以下为本书中所使用的图标示例。


接入交换机


固化汇聚交换机


模块化汇聚交换机


核心交换机


二层堆栈交换机


三层堆栈交换机

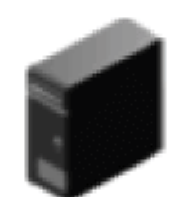

中低端路由器


高端路由器


Voice 多业务路由器


SOHO 多业务路由器


IPv6 多业务路由器


服务器


单路 AP


双路 AP


无线网卡 1


无线网卡 2


无线网桥


无线交换机



感谢提供网络产品和方案的锐捷网络有限公司，为全书提供多个来自不同行业的工程案例。为方便对工程项目的技术细节诠释，本书技术描述主要依托锐捷网络 RGNOS 网络操作系统展开。但在书籍中出现的所有命令和术语，同样具有通用性，能兼容目前网络工程施工中应用到的所有主流设备。并且本书中讲述的技术原理，以及针对网络问题提出的解决方案，同样可以适用于所有现实网络工作场景。

尽管得到了众多一线授课教师及业内专家建议，但面对复杂的工程选择，繁杂网络技术描述，以及把工程和技术完美结合的编撰工作，创新教材编辑委员会深知仍然难免有所错漏，还望读者批评指正。

同时也欢迎读者多提宝贵意见，邮件请发至 labserv@ruijie. com. cn。

目 录

第 1 章 基于路由器 VPN 安全

1.1 使用路由器构建站点到站点 IPSec VPN

【实验名称】

使用路由器构建站点到站点 IPSec VPN。

【实验目的】

学习在路由器上配置站点到站点(Site-to-Site)IPSec(IP security,IPSec)VPN 隧道,加深对 IPSec 理解。

【背景描述】

北京的某公司在上海设立了分公司,分公司要远程访问总公司的各种网络资源,如 CRM 系统、FTP 服务器等。公司担心直接在 Internet 上传输公司内部数据本身存在安全隐患,希望通过 IPSec VPN 技术,实现数据的安全传输。

【需求分析】

需求:解决上海分公司和北京总公司之间,通过 Internet 进行数据传输的安全问题。

分析:IPSec VPN 技术通过隧道技术、加解密技术、密钥管理技术、认证技术等,有效地保证了数据在 Internet 传输的安全性,是目前最安全、使用最广泛的 VPN 技术。因此通过在通信双方建立 IPSec VPN 的加密隧道,实现分公司和总公司之间数据的安全传输。

【实验拓扑】

如图 1-1 所示网络拓扑,是某公司为解决上海分公司和北京总公司之间,通过 Internet 进行数据传输的安全问题。分公司要远程访问总公司的各种网络资源,需要在 Internet 上传输数据,公司希望通过在双方接入路由器上,配置站点到站点(Site-to-Site)的 IPSec VPN 隧道技术,实现数据在 Internet 上的安全传输。

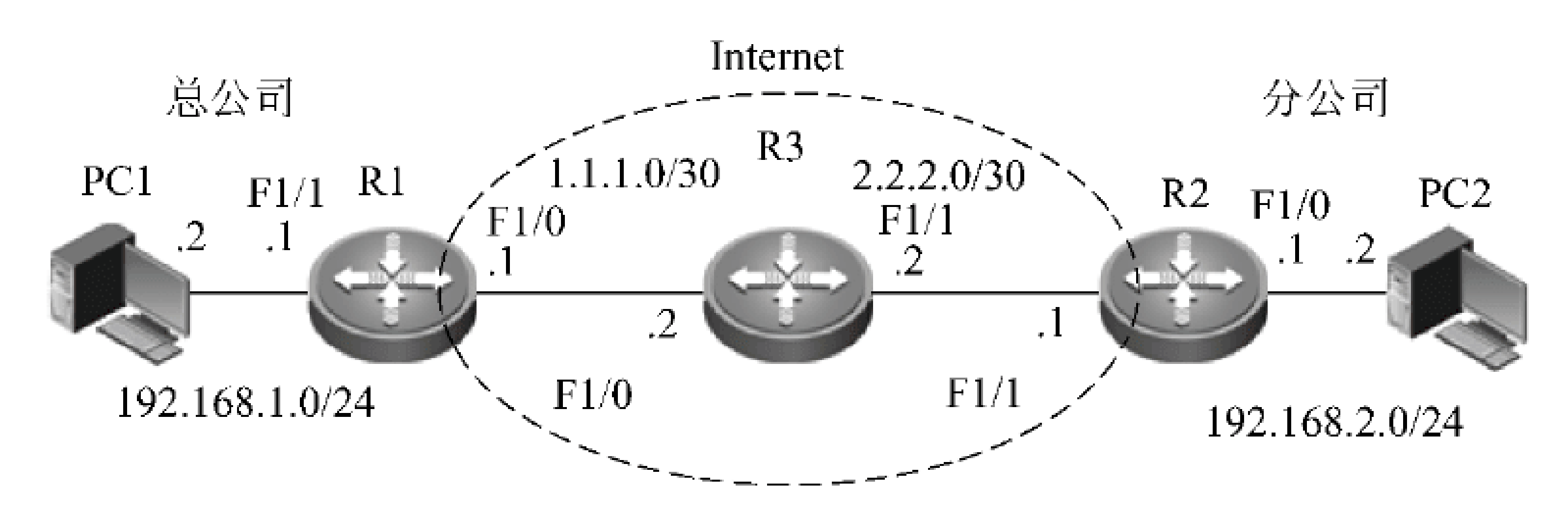


图 1-1 构建站点到站点 IPSec VPN 网络拓扑

【实验设备】

路由器：3 台；PC：2 台。

【预备知识】

VPN 基础知识

VPN(Virtual Private Network)即虚拟专用网技术，所谓虚拟是指用户不需要拥有实际的长途数据线路，而是使用 Internet 公众数据网络的长途数据线路。所谓专用网络指用户可以为自己制定一个最符合自己需求的网络。

虚拟专用网不是真正的专用网络，却能够实现专用网络的功能。VPN 虚拟专网技术在 Internet 公共网络中建立私有专用网络，企业内部保密的数据通过在公网上建立的安全的“加密管道”，在公共网络中传播。

虚拟专用网中的数据通过安全“加密管道”在公共网络中传播，企业只需要租用本地的数据专线，或者用户拨号方式连接上本地的公共信息网，就可以互相传递信息，实现分散地点间的企业内部用户，安全地连接进入远程企业网中，从而实现安全数据传输的目的。IETF 草案理解基于 IP 的 VPN 为：“使用 IP 机制仿真出一个私有的广域网”，通过私有的隧道技术，在公共数据网络上仿真一条点到点的专线技术。

VPN 技术的出现，使企业不再依赖于昂贵的长途拨号以及长途专线服务，而代之以本地 ISP 提供的 VPN 服务。从企业中心站点铺设至当地 ISP 的专线，要比传统 WAN 解决方案中长途专线短得多，成本也低廉得多。

Internet 所具备的高带宽、低费用以及无限连接特性，对企业具有极大的诱惑性，但 Internet 本身所具有的开放性和松散管理特征，也使企业面临的网络安全问题更加尖锐，此问题成了 Internet 作为商务网络必须跨越的重大障碍。而虚拟专用网 VPN 技术，可以防止数据在公网传输中被窃听；防止数据在公网传输中被篡改；可以验证数据的真实来源；成本低廉(相对于专线、长途拨号)；应用灵活、可扩展性好，是目前和今后一段时间内，企业构建广域网络的发展趋势，它逐步成为实现企业网络跨地域安全互联的主要技术手段。

有了 VPN，用户在家里或在路途中，就可以利用 Internet 公共网络，对企业内部服务器进行远程安全访问。从用户的角度来看，VPN 就是在用户计算机(VPN 客户机)和企业服务器(VPN 服务器)之间点到点的连接。由于数据通过一条仿真专线传输，用户感觉不到公共网络的实际存在，像在专线上一样处理企业内部信息。

VPN 可以广泛应用于各个领域，使企业通过公共网络在公司总部和各远程分部，以及客户之间建立快捷、安全、可靠的通信。这种连接方式在概念上等同于传统广域网。在满足基本应用要求后，有 3 类用户比较适合采用 VPN。

(1) 位置众多，特别是单个用户和远程办公室站点多，例如，企业用户、远程教育用户；

(2) 用户/站点分布范围广，彼此之间的距离远，遍布全球各地，需通过长途电信，甚至国际长途手段联系的用户；

(3) 带宽和时延要求相对适中的用户；

(4) 对线路保密性有一定要求的用户。

相对而言,以下 4 种情况可能并不适于采用 VPN:

(1) 非常重视传输数据的安全性;

(2) 不管价格多少,性能都被放在第一位的情况;

(3) 采用不常见的协议,不能在 IP 隧道中传送应用的情况;

(4) 大多数通信是实时通信的应用,如语音和视频。

IPSec 工作原理

由于需要在 Internet 上传输公司内部的私有信息,VPN 用户对数据的安全性都比较关心,安全问题是 VPN 的核心问题。目前 VPN 主要采用四项技术来保证安全,这四项技术分别是隧道技术(Tunneling)、加解密技术(Encryption & Decryption)、密钥管理技术(Key Management)、使用者与设备身份认证技术(Authentication)。通过这四项安全技术来保证企业远程办公员工安全访问公司内部网络。

其中隧道技术是 VPN 的基本技术,类似于点对点连接技术,它在公用网建立一条专用数据通道(隧道),让数据包通过这条隧道传输。隧道由隧道协议形成,分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中,再把整个数据包装入隧道协议中,双层封装形成的数据包通过第二层协议进行传输。常见的第二层隧道协议有 L2F、PPTP、L2TP 等。其中 L2TP 协议由 PPTP 与 L2F 融合而形成。第三层隧道协议是把各种网络协议,直接装入隧道协议中,形成的数据包依靠第三层协议进行传输,其中第三层隧道协议有 VTP、IPSec 等。IPSec(IP Security)是最常见第三层隧道协议,由一组 RFC 文档组成,定义了一个系统来提供安全协议选择、安全算法,确定服务所使用密钥等服务,从而在 IP 层提供安全保障。

Internet Protocol Security(IPSec)是由 Internet Engineering Task Force(IETF)组织定义的安全标准框架,是保护 IP 协议安全通信的标准。它主要对 IP 协议分组进行加密和认证,用以提供公用和专用网络的端对端加密和验证服务。IPSec 具有互操作性、高质量、基于加密特征,适用于 IPv4 和 IPv6 的协议规范。IPSec 能够对数据的存取控制、机密性、完整性和可用性提供保证,并能够防止重放攻击。IPSec 可应用在 IP 层对 IP 包进行封装,或在 IP 层与数据链路层之间提供安全保障。

IPSec 协议的工作原理类似于包过滤防火墙,可以看做是对包过滤防火墙的一种扩展。当接收到一个 IP 数据包时,包过滤防火墙解析数据包头部信息,把头部信息放在一个规则表中进行匹配。当找到一个相匹配的规则时,包过滤防火墙按照规则制定的策略,对接收到的 IP 数据包进行两种处理——丢弃或转发。而 IPSec 则把头部信息通过查询安全策略数据库(Security Policy Database,SD)来决定对接收到的 IP 数据包的处理。另外不同于包过滤防火墙的处理方法是,IPSec 技术对 IP 数据包的处理方法除了丢弃、直接转发(绕过 IPSec)外,还有一种,即进行 IPSec 安全处理。

IPSec 作为一个协议族(即一系列相互关联的协议)由以下部分组成:

① 保护分组流的协议;

② 用来建立这些安全分组流的密钥交换协议,包括:加密分组流的封装安全载荷协

议(ESP)及较少使用的认证头协议(AH)。

IPSec 是标准的第三层安全协议,用于保护 IP 数据包或上层数据,它可以定义哪些数据流需要保护,怎样保护以及应该将这些受保护的数据流转发给谁。由于它工作在网络层,因此可以用于两台主机之间,实施网络安全网关之间(如防火墙、路由器),或主机与网关之间数据安全。

IPSec 协议由 3 个基本协议提供安全保护:认证协议头(AH)、安全加载封装(ESP)和互联网密匙管理协议(IKMP)。认证协议头和安全加载封装可以通过分开或组合使用,达到所希望的保护等级,用以保护网络安全通信。

IPSec 协议中 ESP 和 AH 安全协议都可以提供网络安全,如数据源认证(确保接收到的数据是来自发送方),数据完整性(确保数据没有被更改)以及防中继保护(确保数据到达次序的完整性)。除此之外,ESP 协议还支持数据的保密性,确保其他人无法读取传送的数据,这实际上是采用加密算法来实现。

IPSec 的安全服务要求支持共享钥匙完成认证或加密。在 IPSec 协议中还引入了一个钥匙管理协议,称 Internet 钥匙交换协议(IKE),该协议可以动态认证 IPSec 对等体,协商安全服务,并自动生成共享钥匙。

IPSec 协议(AH 或 ESP)保护整个 IP 包或 IP 包中的上层协议。IPSec 有两种工作方式:传输方式保护上层协议,如 TCP;隧道方式保护整个 IP 包。在传输方式下,IPSec 包头加在 IP 包头和上层协议包头之间;而在隧道方式下,整个 IP 包都封装在一个新的 IP 包中,并在新的 IP 包头和原来的 IP 包头之间插入 IPSec 头。两种 IPSec 协议 AH 和 ESP 都可以工作在传输方式下或隧道方式下。

认证头(Authentication header, AH)协议被用来保证被传输分组的完整性和可靠性,此外,它还保护不受重发攻击。认证头试图保护 IP 数据报的所有字段(那些在传输 IP 分组的过程中要发生变化的字段被排除在外),实现数据发送方的验证处理。这样就可确保数据既对未经验证的站点不可用,也不能在路由过程中更改。在 AH 传送模式中,验证头将插入 IP 头和负载之间,AH 认证头提供数据源验证处理所需要的安全参数索引、顺序编号以及其他数据。

封装安全载荷(ESP)协议对分组提供了源可靠性、完整性和保密性的支持。与 AH 头不同的是,IP 分组头部不被包括在内。ESP 协议实现了发送方的验证处理和数据加密处理,用以确保数据不会被拦截、查看或复制。在 ESP 传送模式中,ESP 头将插入 IP 头和负载之间,而 ESP 尾和验证 MAC 将添加至数据包末端。在通道模式 ESP 中,整个数据包经过了加密处理,并附加了新的 ESP 头、IP 头和验证尾。IPSec 与其他业界规范相互兼容,IPSec 支持 MD-5 和 SHA-1 等验证代码,并支持 DES 和 3DES 用以进行高级加密处理。

如果在路由器或防火墙上实施了 IPSec 协议,它就会为周边的通信提供强有力的安全保障。IPSec 具有以下一些优点。

(1) IPSec 协议运行在传输层之下,对于上层应用程序来说是透明的。当在路由器或防火墙上安装 IPSec 协议时,无须更改用户或服务器系统中的软件设置。即使在终端系

统中执行 IPSec 协议，应用程序一类的上层软件也不会被影响。

（2）IPSec 协议对终端用户来说是透明的，因此不必对用户进行安全机制的培训。

（3）IPSec 协议可以为个体用户提供网络传输的安全保障，这样做就可以保护企业内部的敏感信息。

【实验原理】

IPSec 安全性主要作用是为 IP 数据通信提供安全服务。IPSec 不是一个单独协议，它是一套完整的体系框架，主要包括 AH、ESP 和 IKE 三个协议。

IPSec 使用了多种加密算法、散列算法、密钥交换方法等为 IP 数据流提供安全性，它可以提供数据的机密性、数据的完整性、数据源认证和反重放等安全服务。

【实验步骤】

第一步：按如图 1-1 所示拓扑，连接实验中网络设备，注意接口上地址规划信息。

第二步：配置 Internet 路由器 R3 接口信息。

```
R3# configure terminal
R3(config)# interface fastEthernet 1/0
R3(config-if)# ip address 1.1.1.2 255.255.255.252
R3(config-if)# exit
R3(config)# interface fastEthernet 1/1
R3(config-if)# ip address 2.2.2.2 255.255.255.252
R3(config-if)# exit
```

第三步：配置 R1 与 R2 的 Internet 连通性。

```
R1# configure terminal
R1(config)# interface fastEthernet 1/0
R1(config-if)# ip address 1.1.1.1 255.255.255.252
R1(config-if)# exit
R1(config)# interface fastEthernet 1/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# exit
R1(config)# ip route 0.0.0.0 0.0.0.0 1.1.1.2

R2# configure terminal
R2(config)# interface fastEthernet f1/1
R2(config-if)# ip address 2.2.2.1 255.255.255.252
R2(config-if)# exit
R2(config)# interface fastEthernet 1/0
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 2.2.2.2
```

第四步：配置 R1 的 IKE 协议。

```
R1(config)# crypto isakmp policy 1                    !创建 IKE 策略
```

```
R1(isakmp-policy)#encryption 3des                          !使用 3DES 加密算法
R1(isakmp-policy)#authentication pre-share                 !使用预共享密钥验证方式
R1(isakmp-policy)#hash sha                                 !使用 SHA-1 算列算法
R1(isakmp-policy)#group 2                                  !使用 DH 组 2
R1(isakmp-policy)#exit
R1(config)#crypto isakmp key 0 1234567 address 2.2.2.1     !配置预共享密钥
```

第五步：配置 R1 的 IPSec 协议。

```
R1(config)#crypto ipsec transform-set 3des_sha esp-3des esp-sha-hmac
        !配置 IPSec 转换集,使用 ESP 协议,3DES 算法和 SHA-1 散列算法
R1(cfg-crypto-trans)#exit
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
        !配置加密访问控制列表
R1(config)#crypto map to_r2 1 ipsec-isakmp              !配置 IPSec 加密映射
R1(config-crypto-map)#match address 100                 !引用加密访问控制列表
R1(config-crypto-map)#set transform-set 3des_sha        !引用 IPSec 转换集
R1(config-crypto-map)#set peer 2.2.2.1                  !配置 IPSec 对等体地址
R1(config-crypto-map)#exit
R1(config)#interface fastEthernet1/0
R1(config-if)#crypto map to_r2                          !将 IPSec 加密映射应用到接口
R1(config-if)#exit
```

第六步：配置 R2 的 IKE 协议。

```
R2(config)#crypto isakmp policy 1
R2(isakmp-policy)#encryption 3des
R2(isakmp-policy)#authentication pre-share
R2(isakmp-policy)#hash sha
R2(isakmp-policy)#group 2
R2(isakmp-policy)#exit
R2(config)#crypto isakmp key 0 1234567 address 1.1.1.1
```

第七步：配置 R2 的 IPSec 协议。

```
R2(config)#crypto ipsec transform-set 3des_sha esp-3des esp-sha-hmac
R2(cfg-crypto-trans)#exit
R2(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#crypto map to_r1 1 ipsec-isakmp
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#set transform-set 3des_sha
R2(config-crypto-map)#set peer 1.1.1.1
R2(config-crypto-map)#exit
R2(config)#interface fastEthernet1/0
R2(config-if)#crypto map to_r1
R2(config-if)#exit
```

第八步：配置 PC1 和 PC2 地址。

```
PC1的 IP地址为 192.168.1.2,网关为 192.168.1.1
PC2的 IP地址为 192.168.2.2,网关为 192.168.2.1
```

第九步：验证测试(1)。

在 PC1 上使用 ping 命令测试和 PC2 连通性，可以 ping 通。由于第一个报文用于触发 IKE 协商并建立 IPSec 隧道，所以第一个 ping 包会由于超时而未得到响应，如图 1-2 所示。

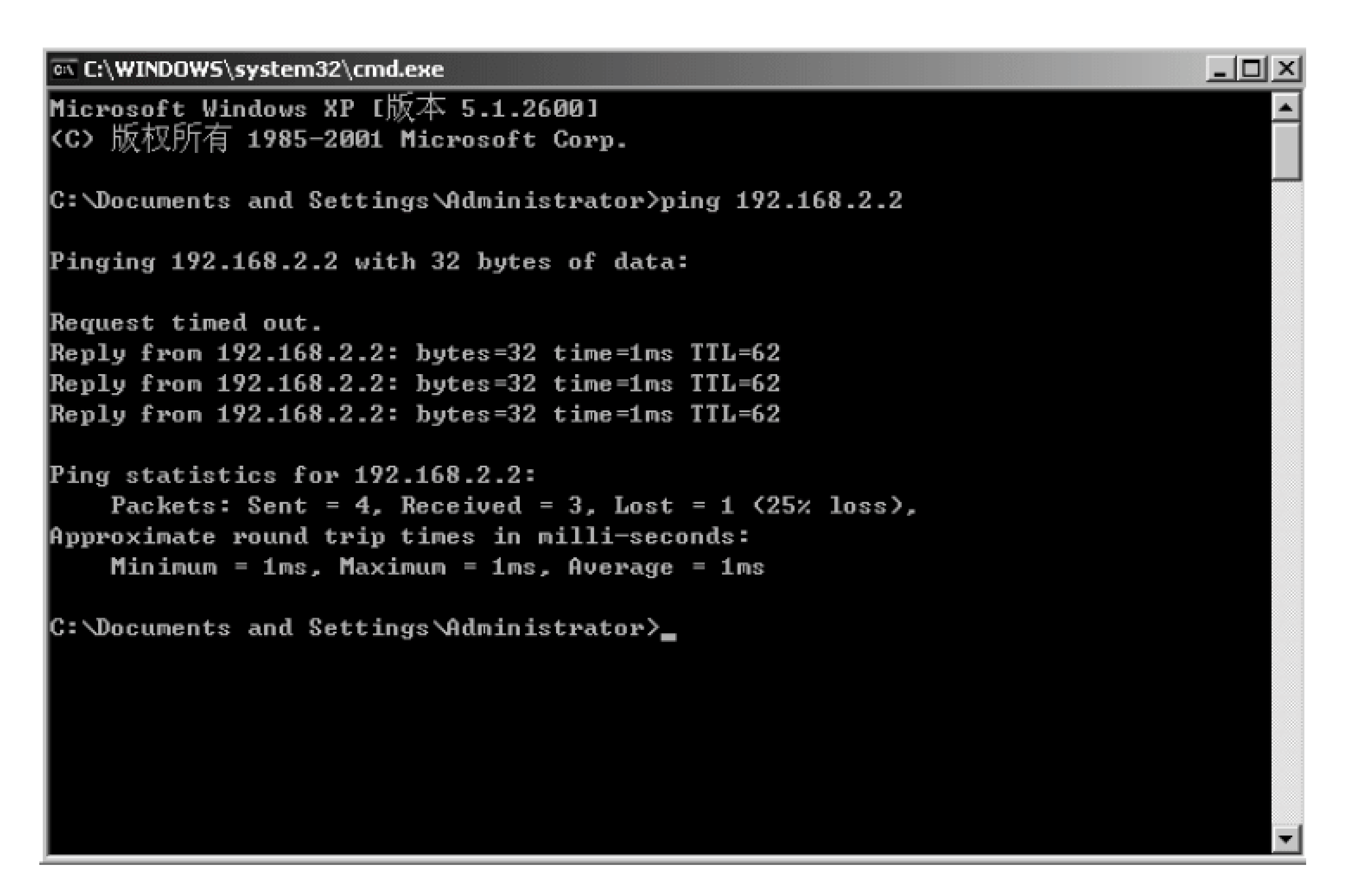


图 1-2　验证测试

第十步：验证测试。

(1) 查看 R1 的 IKE SA，可以看到 IKE SA 协商成功，状态为 QM_IDLE。

```
R1# show crypto isakmp sa
destination    source        state        conn-id          lifetime(second)
2.2.2.1        1.1.1.1       QM_IDLE        33                85896
31c961f99129c159   009f3edd7c1bba59
```

(2) 查看 R1 的 IPSec SA，可以看到两个 IPSec SA 协商成功，一个用于入站报文，一个用于出站报文。

```
R1# show crypto ipsec sa

Interface: FastEthernet 1/0
        Crypto map tag:to_r2, local addr 1.1.1.1
        media mtu 1500

        ==================================================
        item type:static, seqno:1, id=32
        local   ident (addr/mask/prot/port): (192.168.1.0/0.0.0.255/0/0))
        remote  ident (addr/mask/prot/port): (192.168.2.0/0.0.0.255/0/0))
        PERMIT
```

```
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#send errors 0, #recv errors 0

Inbound esp sas:
        spi:0x30098aa2(805931682)
        transform: esp-3des esp-sha-hmac
        in use settings={Tunnel,}
        crypto map to_r2 1
        sa timing: remaining key lifetime(k/sec): (4606999/2933)
        IV size: 8 bytes
        Replay detection support:Y

Outbound esp sas:
        spi:0x1e1e0b3f (505285439)
        transform: esp-3des esp-sha-hmac
        in use settings={Tunnel,}
        crypto map to_r2 1
        sa timing: remaining key lifetime(k/sec): (4606999/2933)
        IV size: 8 bytes
        Replay detection support:Y
```

（3）查看 R2 的 IKE SA，可以看到 IKE SA 协商成功，状态为 QM_IDLE。

```
R2# show crypto isakmp sa
destination    source     state      conn-id      lifetime(second)
2.2.2.1        1.1.1.1    QM_IDLE    33           85618
31c961f99129c159    009f3edd7c1bba59
```

（4）查看 R2 的 IPSec SA，可以看到两个 IPSec SA 协商成功，一个用于入站报文，一个用于出站报文。

```
R2# show crypto ipsec sa

Interface: FastEthernet 1/1
        Crypto map tag:to_r1, local addr 2.2.2.1
        media mtu 1500

        ==================================================
        item type:static, seqno:1, id=32
        local  ident (addr/mask/prot/port): (192.168.2.0/0.0.0.255/0/0))
        remote  ident (addr/mask/prot/port): (192.168.1.0/0.0.0.255/0/0))
        PERMIT
        #pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
        #pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
        #send errors 0, #recv errors 0
```

```
Inbound esp sas:
        spi:0x1e1e0b3f(505285439)
        transform: esp-3des esp-sha-hmac
        in use settings={Tunnel,}
        crypto map to_r1 1
        sa timing: remaining key lifetime(k/sec): (4607999/2785)
        IV size: 8 bytes
        Replay detection support:Y

Outbound esp sas:
        spi:0x30098aa2 (805931682)
        transform: esp-3des esp-sha-hmac
        in use settings={Tunnel,}
        crypto map to_r1 1
        sa timing: remaining key lifetime(k/sec): (4607999/2785)
        IV size: 8 bytes
        Replay detection support:Y
```

通过以上 show 出状态信息可以看出，R1 与 R2 成功协商了一个 IKE SA 和两个 IPSec SA（每个方向各一个）。

【注意事项】

- 双方配置的 IKE 策略和 IPSec 转换集要一致，且双方的预共享密钥要一致。
- 当配置了多个 IKE 策略和 IPSec 转换集时，请确保双方能够协商出一个相同的策略和转换集。
- 双方配置的加密访问列表要互为镜像。

【参考配置】

```
R1# show running-config

Building configuration…
Current configuration: 925 bytes
!
hostname R1
!
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
!
no service password-encryption
!
crypto isakmp policy 1
  encryption 3des
  authentication pre-share
  hash sha
```

```
  group 2
!
crypto isakmp key 7 076f517c41477152 address 2.2.2.1
crypto ipsec transform-set 3des_sha  esp-3des esp-sha-hmac
crypto map to_r2 1 ipsec-isakmp
  set peer 2.2.2.1
  set transform-set 3des_sha
  match address 100
!
interface serial 1/2
  clock rate 64000
!
interface serial 1/3
  clock rate 64000
!
interface FastEthernet 1/0
  ip address 1.1.1.1 255.255.255.252
  crypto map to_r2
  duplex auto
  speed auto
!
interface FastEthernet 1/1
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface Null 0
!
ip route 0.0.0.0 0.0.0.0 1.1.1.2
!
line con 0
line aux 0
line vty 0 4
  login
end
```

R2# show running-config

```
Building configuration...
Current configuration : 925 bytes
hostname R2
access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
!
no service password-encryption
```

```
crypto isakmp policy 1
  encryption 3des
  authentication pre-share
  hash sha
  group 2
!
crypto isakmp key 7 076f517c41477152 address 1.1.1.1
crypto ipsec transform-set 3des_sha  esp-3des esp-sha-hmac
crypto map to_r1 1 ipsec-isakmp
  set peer 1.1.1.1
  set transform-set 3des_sha
  match address 100
!
interface serial 1/2
  clock rate 64000
interface serial 1/3
  clock rate 64000
interface FastEthernet 1/0
  ip address 192.168.2.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet 1/1
  ip address 2.2.2.1 255.255.255.252
  crypto map to_r1
  duplex auto
  speed auto
interface Null 0
!
ip route 0.0.0.0 0.0.0.0 2.2.2.2
!
line con 0
line aux 0
line vty 0 4
  login
end
```

R3# show running-config

```
Building configuration…
Current configuration: 489 bytes
hostname R3
no service password-encryption
interface serial 1/2
```

```
  clock rate 64000
!
interface serial 1/3
  clock rate 64000

interface FastEthernet 1/0
  ip address 1.1.1.2 255.255.255.252
  duplex auto
  speed auto
!
interface FastEthernet 1/1
  ip address 2.2.2.2 255.255.255.252
  duplex auto
  speed auto
interface Null 0
!
line con 0
line aux 0
line vty 0 4
  login
!
End
```

1.2 使用路由器构建 GRE VPN

【实验名称】

使用路由器构建 GRE VPN。

【实验目的】

学习配置站点到站点(Site-to-Site)的 GRE VPN 隧道,加深对 GRE 协议的理解。

【背景描述】

北京的某公司在上海设立了分公司,分公司要能够访问总公司的各种网络资源,如 CRM 系统、FTP 服务器等。由于担心在 Internet 上传输公司共享数据存在安全隐患,公司希望通过 VPN 技术实现总公司和分公司之间的数据安全传输。

【需求分析】

需求:解决上海分公司和北京总公司之间,通过 Internet 进行公司内部保密数据信息传输的安全问题。

分析:GRE VPN 通过隧道技术有效地保证了数据在 Internet 网络上安全地传输,并且 GRE VPN 技术支持对网络上组播和广播数据的封装传输,还可用于封装路由协议报

文，保证安全传输。

【实验拓扑】

如图 1-3 所示网络拓扑，是某公司在上海设立了新的分公司，分公司要远程访问总公司内网中的各种网络资源，实现分公司和总公司之间内部信息共享。为解决上海分公司和北京总公司之间，通过 Internet 进行数据传输的安全问题，公司希望通过 GRE VPN 技术，采用隧道加密功能，有效保证数据在 Internet 传输的安全。

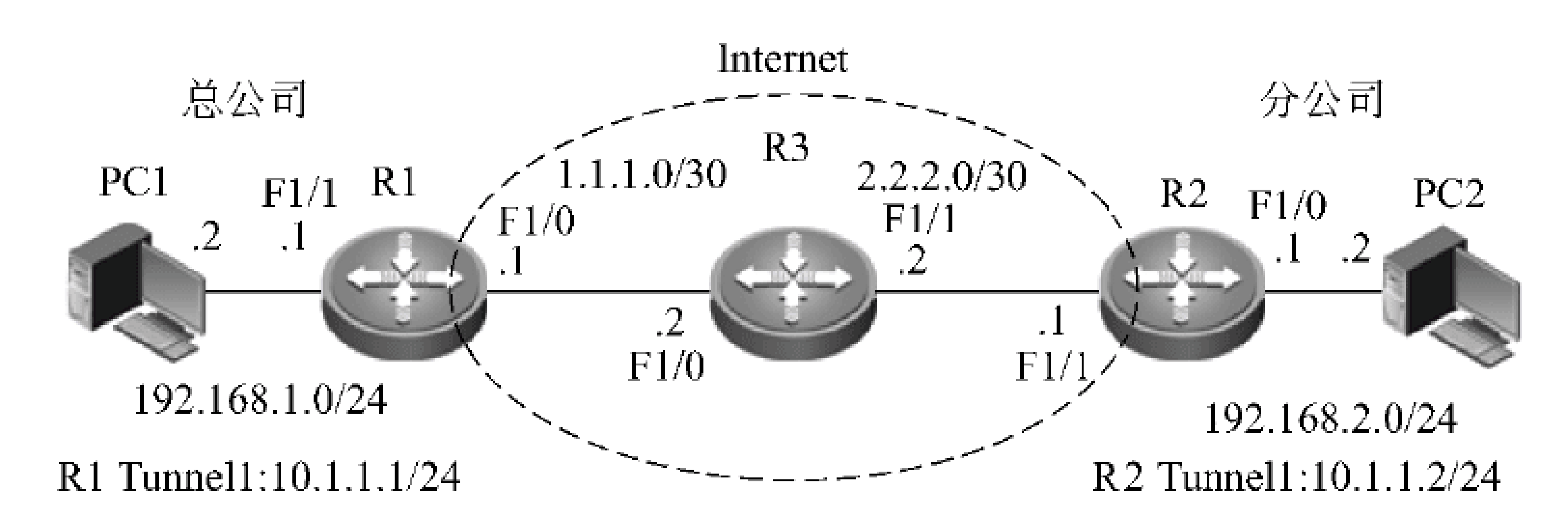


图 1-3　路由器构建 GRE VPN 网络拓扑

【实验设备】

路由器：3 台；PC：2 台。

【预备知识】

GRE 工作原理

VPN 隧道协议主要有三种：PPTP、L2TP 和 IPSec，其中 PPTP 和 L2TP 协议是工作在 OSI/RM 开放模型中的第二层，所以又称之为第二层隧道协议。在 VPN 网络中最常见的第三层隧道协议是 IPSec，但另一种通用路由封装协议（Generic Routing Encapsulation，GRE，在 RFC 1701 中有描述）也属于第三隧道协议。

GRE 通用路由封装定义了在任意一种网络层协议上，封装任意一个其他网络层协议工作机制，是一个在网络层之间传输数据包的通道协议。也就是说，通用路由封装协议是对某些网络层协议（如 IP 和 IPX）的数据包进行封装，使这些被封装的数据包能够在另一个网络层协议（如 IP）中安全传输。GRE 是 VPN 的第三层隧道协议，即在协议层之间采用了一种被称之为 Tunnel（隧道）的技术。

GRE 通用路由封装技术和 IPSec 类似，将 IP 数据包加上 GRE 头，封装在 IP 数据包内，但最大不同是，允许用户使用 IP 协议封装 IP 包、IPX 包和 AppleTalk 包，并支持全部的路由协议（如 RIP2、OSPF 等），但对这些数据包不进行任何的加密和认证，而 IPSec 协议只能封装 IP 数据包。

GRE 隧道协议的配置一般会启用一个隧道接口，在该接口中可以预先定义好该隧道的起点，也就是 GRE 数据包的源 IP 地址，以及隧道的终点，也就是 GRE 数据包的目的地址。在路由器看来 GRE 隧道是一个点到点端口，它可以被加密。网络服务提供商 ISP 可以对 GRE 隧道提供 QoS 服务，但这个隧道的两端必须在同一个 ISP 的网络内。

这里的隧道是指将一种协议封装到另一种协议中。在隧道入口处，将被封装协议封装入封装协议，在隧道出口处再将被封装协议报文取出。在整个隧道的传输过程中，被封

装协议是作为封装协议的负载。隧道技术只需要在隧道的出入口进行修改，而对中间部分没有特殊要求，较为容易实现。

一个报文要想在隧道中传输，必须要经过加封装与解封装两个过程。在大多数情况下，系统拥有一个有效载荷（或负载）包，需要将它封装并发送至某个目的地。首先将有效载荷封装在一个 GRE 包中，然后将此 GRE 包封装在其他某协议并进行转发。

解封装过程和加封装的过程相反。从隧道接口收到的 IP 报文，通过检查目的地址，发现目的地就是此路由器时，剥掉 IP 报头，再交给 GRE 协议处理后（进行检验密钥、检查校验和或报文的序列号等），剥掉 GRE 报头后，再交给和对端一样的协议，对此数据包进行处理。系统收到一个需要封装和路由的数据包，称之为净荷（Payload），这个净荷首先被加上 GRE 封装，成为 GRE 报文；再被封装在 IP 报文中，这样就可完全由 IP 层负责此报文的向前传输。这个负责向前传输的 IP 协议被称为传递（Delivery）协议或传输（Transport）协议。

下面以传输头为 IP 报头为例来介绍 GRE 协议工作过程。

在由 GRE 协议构建的虚拟专用网中，GRE 协议会在总部和分支结构之间建立一条 Tunnel（是一条逻辑链路），隧道通过两端的源 IP 地址和目的 IP 地址定义，私有数据会通过这条 Tunnel 进行传输。

数据在发送端进行加密。数据包在由总部向分支企业发送时，出口路由器通过数据包的目的地址，在路由表中确认此数据包在传输中需要通过虚拟专用网建立的 Tunnel，将数据包发送到 Tunnel 接口，Tunnel 口对数据包进行 GRE 封装，然后再打上 IP 报头，查询路由表，将数据包发送出去。

封装好的数据包在向目的网络传输的过程中，途径的网络设备按照数据包外层的 IP 包头特征信息进行数据转发，在接收端进行解密。接收端接收到数据包后，去掉数据包外部的 IP 包头，然后再去掉内层的 GRE 封装协议，获得原始数据。

简单地说就是，本地网络中设备将企业内部的私有数据进行“伪装”，使其成为另外一种协议的数据分组，然后传送到目的地。目的地接收信息的网络设备去掉数据的“伪装”，露出内部真正要接收的有效载荷。

此外，发送协议 IPv4 被作为 GRE 有效载荷承载的传输协议时，协议类型字段必须被设置为 0x800。当一个隧道终点设备，拆封此含有 IPv4 包作为有效载荷的 GRE 包传输协议时，IPv4 包头中的目的地址必须用来转发包，并且需要减少有效载荷包的 TTL。值得注意的是，在转发这样一个包时，如果有效载荷包中目的地址就是包的封装器（也就是隧道另一端），就会出现回路现象，在此情形下，必须丢弃该包。

GRE VPN 技术下的网络安全的检查过程，与目前常规的 IPv4 网络安全检查过程基本相似，GRE 隧道协议下的路由，仍采用 IPv4 数据包中原本使用的路由，且路由在网络上过滤过程保持不变。在包过滤安全机制下，通过在接收端防火墙上配置检查 GRE 隧道协议封装的数据包，也可在配置 GRE 隧道终点防火墙上完成过滤过程。为加快数据包的通信过程，在一些安全的网络环境下，可以在防火墙上终止隧道协议。

GRE 隧道技术的应用范围为：

① 多协议本地网中数据需要通过单一协议骨干网传输。

② 扩大包含步跳数受限协议(如 IPX)的网络的工作范围。

③ 将一些不能连续的子网连接起来,组建 VPN。

其中以第一种应用为主。

GRE 隧道技术的基本配置,包括创建虚拟 Tunnel 接口、配置 Tunnel 接口的源端地址、配置 Tunnel 接口的目的地址、配置 Tunnel 接口的网络地址。常见的配置命令有:

```
Router#
Router# config terminal
Router(config)# interface tunnel1                        !创建虚拟 Tunnel 接口
Router(config-if)# lip address 10.1.1.1 255.255.255.0
Router(config-if)# tunnel source fastEthernet1/0
!配置隧道的源接口或源地址
Router 1(config-if)# tunnel destination 2.2.2.1          !配置隧道的目的地址
Router (config-if)# tunnel key 1234567                   !配置隧道验证密钥
Router (config-if)# exit
```

【实验原理】

GRE 协议是一个隧道协议,使用 IP 协议号 47。GRE 通常用来构建站点到站点的 VPN 隧道,它最大的优点是可以对多种协议、多种类型的报文进行封装,并封装在隧道中安全传输。但是 GRE 不提供对数据的保护(如加密),它只提供简单的隧道验证功能。

【实验步骤】

第一步:按照如图 1-3 所示拓扑,连接实验中的网络设备,注意接口上地址规划信息。

第二步:配置 Internet 路由器 R3。

```
R3# configure terminal
R3(config)# interface fastEthernet 1/0
R3(config-if)# ip address 1.1.1.2 255.255.255.252
R3(config-if)# exit
R3(config)# interface fastEthernet 1/1
R3(config-if)# ip address 2.2.2.2 255.255.255.252
R3(config-if)# exit
```

第三步:配置 R1 与 R2 的 Internet 连通性。

```
R1# configure terminal
R1(config)# interface fastEthernet 1/0
R1(config-if)# ip address 1.1.1.1 255.255.255.252
R1(config-if)# exit
R1(config)# interface fastEthernet 1/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# exit
```

```
R1(config)# ip route 0.0.0.0 0.0.0.0 1.1.1.2

R2# configure terminal
R2(config)# interface fastEthernet f1/1
R2(config-if)# ip address 2.2.2.1 255.255.255.252
R2(config-if)# exit
R2(config)# interface fastEthernet 1/0
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 2.2.2.2
```

第四步：配置 R1 的 GRE 隧道。

```
R1(config)# interface tunnel1
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# tunnel source fastEthernet1/0        !配置隧道的源接口或源地址
R1(config-if)# tunnel destination 2.2.2.1           !配置隧道的目的地址
R1(config-if)# tunnel key 1234567                   !配置隧道验证密钥
R1(config-if)# exit
```

第五步：在 R1 上启用 RIPv2 路由协议。

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# no auto-summary
R1(config-router)# network 10.0.0.0                 !在 GRE 隧道接口启用 RIPv2
R1(config-router)# network 192.168.1.0              !在内部接口启用 RIPv2
R1(config-router)# exit
```

第六步：配置 R2 的 GRE 隧道。

```
R2(config)# interface tunnel1
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# tunnel source fastEthernet1/1        !配置隧道的源接口或源地址
R2(config-if)# tunnel destination 1.1.1.1           !配置隧道的目的地址
R2(config-if)# tunnel key 1234567                   !配置隧道验证密钥
R2(config-if)# exit
```

第七步：在 R2 上启用 RIPv2 路由协议。

```
R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# no auto-summary
R2(config-router)# network 10.0.0.0                 !在 GRE 隧道接口启用 RIPv2
R2(config-router)# network 192.168.2.0              !在内部接口启用 RIPv2
R2(config-router)# exit
```

第八步：配置测试计算机 PC1 和 PC2。

```
PC1 的 IP 地址为 192.168.1.2 255.255.255.0,网关为 192.168.1.1
PC2 的 IP 地址为 192.168.2.2 255.255.255.0,网关为 192.168.2.1
```

第九步：验证测试 1。

在 R1 与 R2 上验证 GRE 隧道状态及路由表信息，分别通过 Tunnel 接口学习到对端局域网的路由。

```
R1# show interface Tunnel 1

Tunnel 1 is UP  , line protocol is UP                    !隧道状态为 UP
Hardware is  Tunnel
Interface address is: 10.1.1.1/24
  MTU 1472 bytes, BW 9 Kbit
  Encapsulation protocol is Tunnel, loopback not set
  Keepalive interval is 0 sec , no set
  Carrier delay is 0 sec
  RXload is 1 ,Txload is 1
  Tunnel source 1.1.1.1 (FastEthernet 1/0), destination 2.2.2.1
  Tunnel protocol/transport GRE/IP, key 0x12d687, sequencing disabled
  Checksumming of packets disabled  Queueing strategy: WFQ
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 12 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    19 packets output, 988 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets

R1# show ip route

Codes: C- connected, S- static,  R- RIP
       O- OSPF, IA- OSPF inter area
       N1- OSPF NSSA external type 1, N2- OSPF NSSA external type 2
       E1- OSPF external type 1, E2- OSPF external type 2
        * - candidate default

Gateway of last resort is 1.1.1.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 1.1.1.2
C     1.1.1.0/30 is directly connected, FastEthernet 1/0
C     1.1.1.1/32 is local host.
C     10.1.1.0/24 is directly connected, Tunnel 1
C     10.1.1.1/32 is local host.
C     192.168.1.0/24 is directly connected, FastEthernet 1/1
```

```
C      192.168.1.1/32 is local host.
R      192.168.2.0/24 [120/1] via 10.1.1.2, 00:00:29, Tunnel 1

R2# show interface Tunnel 1

Tunnel 1 is UP  , line protocol is UP                          !隧道状态为 UP
Hardware is   Tunnel
Interface address is: 10.1.1.2/24
  MTU 1472 bytes, BW 9 Kbit
  Encapsulation protocol is Tunnel, loopback not set
  Keepalive interval is 0 sec , no set
  Carrier delay is 0 sec
  RXload is 1 ,Txload is 1
  Tunnel source 2.2.2.1 (FastEthernet 1/1), destination 1.1.1.1
  Tunnel protocol/transport GRE/IP, key 0x12d687, sequencing disabled
  Checksumming of packets disabled   Queueing strategy: WFQ
  5 minutes input rate 31 bits/sec, 0 packets/sec
  5 minutes output rate 36 bits/sec, 0 packets/sec
    55 packets input, 3700 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    58 packets output, 4080 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets

R2# show ip route

Codes: C- connected, S- static,   R- RIP
       O- OSPF, IA- OSPF inter area
       N1- OSPF NSSA external type 1, N2- OSPF NSSA external type 2
       E1- OSPF external type 1, E2- OSPF external type 2
        * - candidate default

Gateway of last resort is 2.2.2.2 to network 0.0.0.0
S*     0.0.0.0/0 [1/0] via 2.2.2.2
C      2.2.2.0/30 is directly connected, FastEthernet 1/1
C      2.2.2.1/32 is local host.
C      10.1.1.0/24 is directly connected, Tunnel 1
C      10.1.1.2/32 is local host.
R      192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:20, Tunnel 1
C      192.168.2.0/24 is directly connected, FastEthernet 1/0
C      192.168.2.1/32 is local host.
```

第十步：验证测试 2。

在 PC1 上使用 ping 命令 ping 对端计算机 PC2，可以 ping 通，如图 1-4 所示。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=1ms TTL=62
Reply from 192.168.2.2: bytes=32 time=1ms TTL=62
Reply from 192.168.2.2: bytes=32 time=1ms TTL=62
Reply from 192.168.2.2: bytes=32 time=1ms TTL=62

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

图 1-4 验证测试

【注意事项】

- GRE 隧道两端的密钥要匹配。
- 隧道两端的源和目的相互对应，即 R1 的源地址为 R2 的目的地址，R2 的源地址为 R1 的目的地址。
- 需要在 Tunnel 接口启用路由，而非连接 Internet 的接口。

【参考配置】

```
R1# show running-config

Building configuration...
Current configuration : 764 bytes
!
hostname R1
!
no service password-encryption
!
interface serial 1/2
  clock rate 64000
!
interface serial 1/3
  clock rate 64000
!
interface FastEthernet 1/0
  ip address 1.1.1.1 255.255.255.252
  duplex auto
  speed auto
!
interface FastEthernet 1/1
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
```

```
!
interface Tunnel 1
  ip address 10.1.1.1 255.255.255.0
  tunnel source FastEthernet 1/0
  tunnel destination 2.2.2.1
  tunnel key 1234567
  no keepalive
!
interface Null 0
!
!
router rip
  no auto- summary
  version 2
  network 10.0.0.0
  network 192.168.1.0
!
ip route 0.0.0.0 0.0.0.0 1.1.1.2
!
line con 0
line aux 0
line vty 0 4
  login
end
R2# show running- config

Building configuration…
Current configuration : 764 bytes
!
hostname R2
!
no service password- encryption
!
interface serial 1/2
  clock rate 64000
!
interface serial 1/3
  clock rate 64000
!
interface FastEthernet 1/0
  ip address 192.168.2.1 255.255.255.0
  duplex auto
  speed auto
!
```

```
interface FastEthernet 1/1
  ip address 2.2.2.1 255.255.255.252
  duplex auto
  speed auto
!
interface Tunnel 1
  ip address 10.1.1.2 255.255.255.0
  tunnel source FastEthernet 1/1
  tunnel destination 1.1.1.1
  tunnel key 1234567
  no keepalive
!
interface Null 0
!
router rip
  no auto-summary
  version 2
  network 10.0.0.0
  network 192.168.2.0
!
ip route 0.0.0.0 0.0.0.0 2.2.2.2
!
line con 0
line aux 0
line vty 0 4
  login
!
!
end

R3# show running-config

Building configuration…
Current configuration : 489 bytes
hostname R3
!
no service password-encryption
!
interface serial 1/2
  clock rate 64000
!
interface serial 1/3
  clock rate 64000
!
```

```
interface FastEthernet 1/0
  ip address 1.1.1.2 255.255.255.252
  duplex auto
  speed auto
!
interface FastEthernet 1/1
  ip address 2.2.2.2 255.255.255.252
  duplex auto
  speed auto
interface Null 0
!
line con 0
line aux 0
line vty 0 4
  login
!
!
End
```

1.3 使用路由器构建 GRE over IPSec VPN

【实验名称】

使用路由器构建 GRE over IPSec VPN。

【实验目的】

学习配置站点到站点(Site-to-Site)的 GRE over IPSec VPN，加深对 GRE 与 IPSec 的理解。

【背景描述】

北京的某公司在上海开了新的分公司，分公司要远程访问总公司的各种内部网络资源，例如：CRM 系统、FTP 服务器等。公司担心在 Internet 上传输公司内部保密数据存在安全隐患，希望通过 IPSec VPN 技术实现数据在公共网络上的安全传输。由于总公司和分公司之间需要共享路由信息，所以还要使用 GRE。

【需求分析】

需求：解决上海分公司和北京总公司之间，通过 Internet 公网进行路由信息共享和保密信息安全传输的问题。

分析：IPSec VPN 技术通过隧道技术、加解密技术、密钥管理技术和认证技术有效地保证了数据在 Internet 网络传输的安全性，是目前最安全、使用最广泛的 VPN 技术。由于 GRE 技术支持对网络中组播和广播数据的安全封装，可用于封装路由协议报文。因此可以通过建立 GRE over IPSec VPN 的加密隧道，实现分公司和总公司之间的路由信

息共享和信息安全传输双重功能。

【实验拓扑】

如图 1-5 所示网络拓扑，是上海设立新的分公司要远程访问总公司的各种网络资源，实现分公司和总公司之间信息共享网络场景。为解决上海分公司和北京总公司之间，通过 Internet 进行数据传输的安全问题，公司希望通过 GRE VPN 技术，使用路由器构建 GRE over IPSec VPN 功能，有效保证保密数据在 Internet 网络上安全传输。

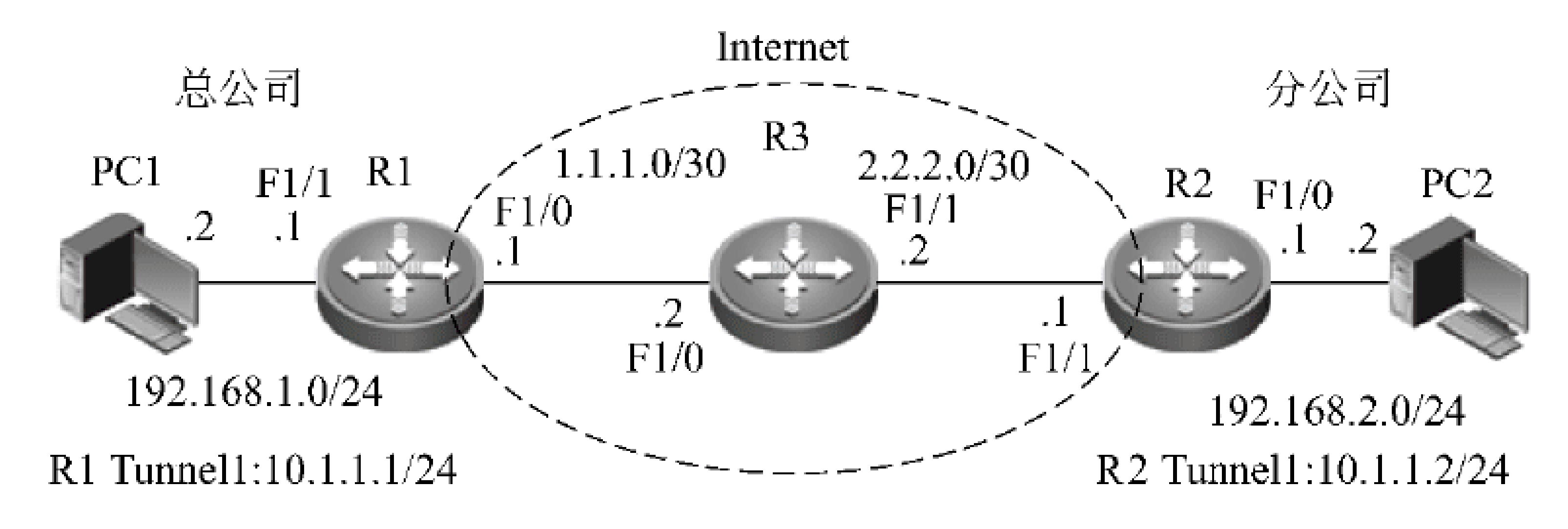


图 1-5 路由器构建 GRE over IPSec VPN 网络拓扑

【实验设备】

路由器：3 台；PC：2 台。

【实验原理】

GRE 协议是一个隧道封装协议，使用 IP 协议号 47。GRE 通常用来构建站点到站点的 VPN 隧道，它最大的优点是可以对多种协议、多种类型的报文进行封装，并在隧道中传输。但是 GRE 不提供对数据的保护(例如，加密)，它只提供简单的隧道验证功能。

IPSec 的主要作用是为 IP 数据通信提供安全服务。IPSec 不是一个单独协议，它是一套完整的体系框架，包括 AH、ESP 和 IKE 三个协议。IPSec 使用了多种加密算法、散列算法、密钥交换方法等为 IP 数据流提供安全性，它可以提供数据的机密性、数据的完整性、数据源认证和反重放等安全服务。

由于 IPSec 不能够对网络中组播报文进行封装，所以常用的路由协议报文无法在 IPSec 协议封装隧道中传输。这时可以结合使用 GRE 与 IPSec 两种技术，利用 GRE 技术对用户数据和路由协议报文进行隧道封装，然后使用 IPSec 技术来保护 GRE 隧道的安全，即构成了 GRE over IPSec VPN 技术。

【实验步骤】

第一步：按如图 1-5 所示拓扑，连接实验中的网络设备，注意接口上地址信息。

第二步：配置 Internet 路由器 R3。

```
R3# configure terminal
R3(config)# interface fastEthernet 1/0
R3(config-if)# ip address 1.1.1.2 255.255.255.252
R3(config-if)# exit
R3(config)# interface fastEthernet 1/1
```

```
R3(config-if)# ip address 2.2.2.2 255.255.255.252
R3(config-if)# exit
```

第三步：配置 R1 与 R2 的 Internet 连通性。

```
R1# configure terminal
R1(config)# interface fastEthernet 1/0
R1(config-if)# ip address 1.1.1.1 255.255.255.252
R1(config-if)# exit
R1(config)# interface fastEthernet 1/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# exit
R1(config)# ip route 0.0.0.0 0.0.0.0 1.1.1.2

R2# configure terminal
R2(config)# interface fastEthernet f1/1
R2(config-if)# ip address 2.2.2.1 255.255.255.252
R2(config-if)# exit
R2(config)# interface fastEthernet 1/0
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 2.2.2.2
```

第四步：配置 R1 的 GRE 隧道。

```
R1(config)# interface tunnel1
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# tunnel source fastEthernet1/0          !配置隧道的源接口或源地址
R1(config-if)# tunnel destination 2.2.2.1             !配置隧道的目的地址
R1(config-if)# tunnel key 1234567                     !配置隧道验证密钥
R1(config-if)# exit
```

第五步：在 R1 上启用 RIPv2 路由协议。

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# no auto-summary
R1(config-router)# network 10.0.0.0                   !在 GRE 隧道接口启用 RIPv2
R1(config-router)# network 192.168.1.0                !在内部接口启用 RIPv2
R1(config-router)# exit
```

第六步：配置 R2 的 GRE 隧道。

```
R2(config)# interface tunnel1
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# tunnel source fastEthernet1/1          !配置隧道的源接口或源地址
R2(config-if)# tunnel destination 1.1.1.1             !配置隧道的目的地址
```

```
R2(config-if)#tunnel key 1234567                       !配置隧道验证密钥
R2(config-if)#exit
```

第七步：在 R2 上启用 RIPv2 路由协议。

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 10.0.0.0                     !在 GRE 隧道接口启用 RIPv2
R2(config-router)#network 192.168.2.0                  !在内部接口启用 RIPv2
R2(config-router)#exit
```

第八步：配置 R1 的 IKE 参数。

```
R1(config)#crypto isakmp policy 1                      !创建 IKE 策略
R1(isakmp-policy)#encryption 3des                      !使用 3DES 加密算法
R1(isakmp-policy)#authentication pre-share             !使用预共享密钥验证方式
R1(isakmp-policy)#hash sha                             !使用 SHA-1 算列算法
R1(isakmp-policy)#group 2                              !使用 DH 组 2
R1(isakmp-policy)#exit
R1(config)#crypto isakmp key 0 1234567 address 2.2.2.1 !配置预共享密钥
```

第九步：配置 R1 的 IPSec 参数。

```
R1(config)#crypto ipsec transform-set 3des_sha esp-3des esp-sha-hmac
!配置 IPSec 转换集,使用 ESP 协议,3DES 算法和 SHA-1 散列算法

R1(cfg-crypto-trans)#mode transport                 !配置 IPSec 工作模式为传输模式

R1(cfg-crypto-trans)#exit
R1(config)#access-list 100 permit 47 host 1.1.1.1 host 2.2.2.1
!配置加密访问控制列表,使用 GRE 协议(47)作为触发流量

R1(config)#crypto map to_r2 1 ipsec-isakmp          !配置 IPSec 加密映射
R1(config-crypto-map)#match address 100             !引用加密访问控制列表
R1(config-crypto-map)#set transform-set 3des_sha    !引用 IPSec 转换集
R1(config-crypto-map)#set peer 2.2.2.1              !配置 IPSec 对等体地址
R1(config-crypto-map)#exit

R1(config)#interface fastEthernet1/0
R1(config-if)#crypto map to_r2                      !将 IPSec 加密映射应用到接口
R1(config-if)#exit
```

第十步：配置 R2 的 IKE 参数。

```
R2(config)#crypto isakmp policy 1
R2(isakmp-policy)#encryption 3des
R2(isakmp-policy)#authentication pre-share
```

```
R2(isakmp-policy)# hash sha
R2(isakmp-policy)# group 2
R2(isakmp-policy)# exit
R2(config)# crypto isakmp key 0 1234567 address 1.1.1.1
```

第十一步：配置 R2 的 IPSec 参数。

```
R2(config)# crypto ipsec transform-set 3des_sha esp-3des esp-sha-hmac
R2(cfg-crypto-trans)# mode transport                    !配置 IPSec 工作模式为传输模式
R2(cfg-crypto-trans)# exit

R2(config)# access-list 100 permit 47 host 2.2.2.1 host 1.1.1.1
!配置加密访问控制列表,使用 GRE 协议(47)作为触发流量

R2(config)# crypto map to_r1 1 ipsec-isakmp
R2(config-crypto-map)# match address 100
R2(config-crypto-map)# set transform-set 3des_sha
R2(config-crypto-map)# set peer 1.1.1.1
R2(config-crypto-map)# exit
R2(config)# interface fastEthernet1/0
R2(config-if)# crypto map to_r1
R2(config-if)# exit
```

第十二步：配置 PC1 和 PC2。

PC1 的 IP 地址为 192.168.1.2 255.255.255.0,网关为 192.168.1.1
PC2 的 IP 地址为 192.168.2.2 255.255.255.0,网关为 192.168.2.1

第十三步：验证测试。

在 PC1 上使用测试命令 ping PC2，可以 ping 通对端设备，如图 1-6 所示。测试成功，表示构建 GRE over IPSec VPN 隧道建立成功。

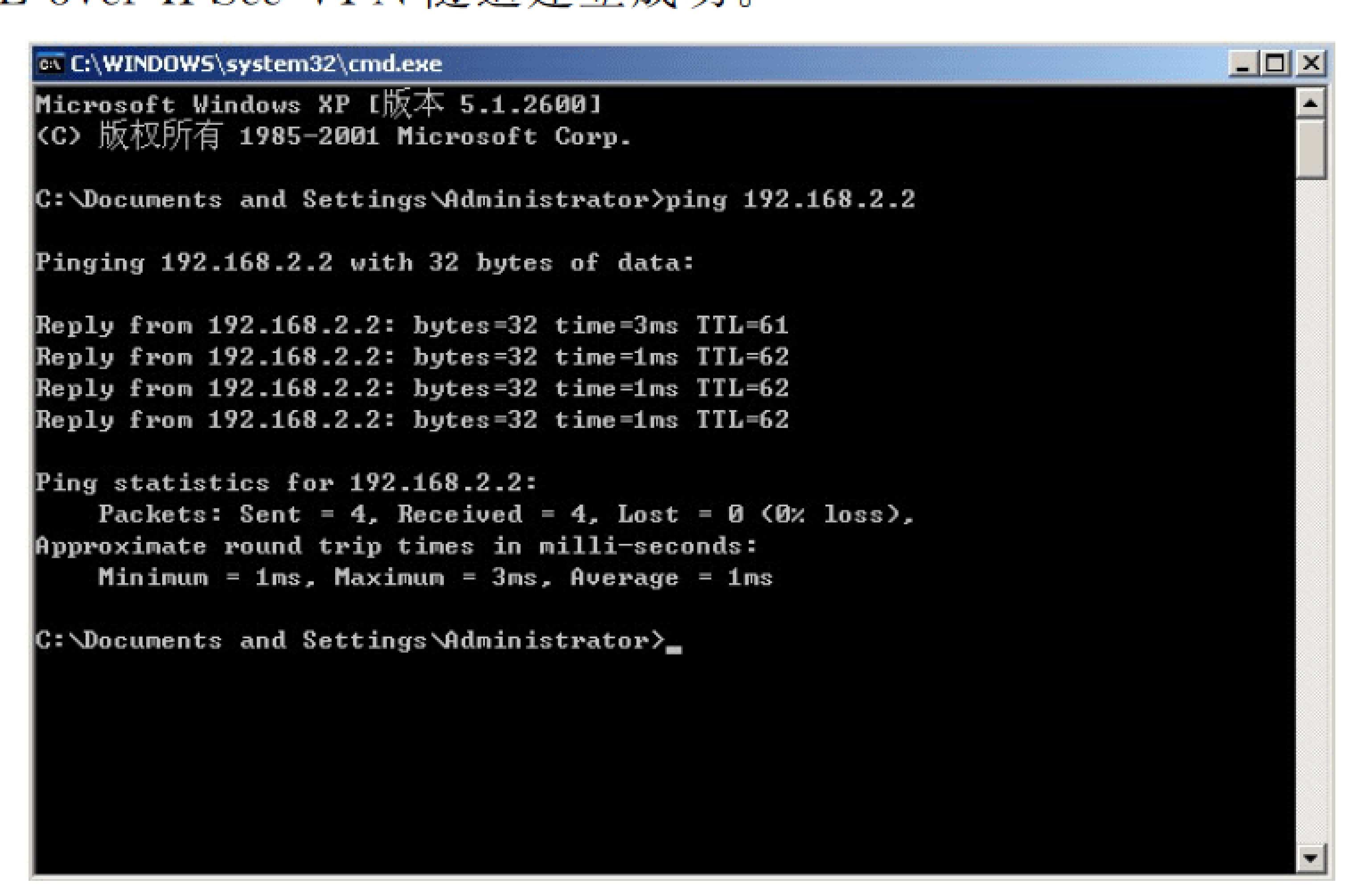


图 1-6　验证测试

第十四步：验证测试。

在 R1 与 R2 上验证 GRE 隧道状态及路由表信息，分别通过 Tunnel 接口学习到对端局域网的路由。

```
R1# show interface Tunnel 1
Tunnel 1 is UP  , line protocol is UP                    !隧道状态为 UP
Hardware is  Tunnel
Interface address is: 10.1.1.1/24
  MTU 1472 bytes, BW 9 Kbit
  Encapsulation protocol is Tunnel, loopback not set
  Keepalive interval is 0 sec , no set
  Carrier delay is 0 sec
  RXload is 1 ,Txload is 1
  Tunnel source 1.1.1.1 (FastEthernet 1/0), destination 2.2.2.1
  Tunnel protocol/transport GRE/IP, key 0x12d687, sequencing disabled
  Checksumming of packets disabled  Queueing strategy: WFQ
  5 minutes input rate 13 bits/sec, 0 packets/sec
  5 minutes output rate 13 bits/sec, 0 packets/sec
    49 packets input, 2580 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    70 packets output, 3756 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets

R1# show ip route

Codes: C- connected, S- static,  R- RIP
       O- OSPF, IA- OSPF inter area
       N1- OSPF NSSA external type 1, N2- OSPF NSSA external type 2
       E1- OSPF external type 1, E2- OSPF external type 2
       * - candidate default

Gateway of last resort is 1.1.1.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 1.1.1.2
C     1.1.1.0/30 is directly connected, FastEthernet 1/0
C     1.1.1.1/32 is local host.
C     10.1.1.0/24 is directly connected, Tunnel 1
C     10.1.1.1/32 is local host.
C     192.168.1.0/24 is directly connected, FastEthernet 1/1
C     192.168.1.1/32 is local host.
R     192.168.2.0/24 [120/1] via 10.1.1.2, 00:00:16, Tunnel 1

R2# show interface tunnel 1
Tunnel 1 is UP  , line protocol is UP                   !隧道状态为 UP
```

```
Hardware is  Tunnel
Interface address is: 10.1.1.2/24
  MTU 1472 bytes, BW 9 Kbit
  Encapsulation protocol is Tunnel, loopback not set
  Keepalive interval is 0 sec , no set
  Carrier delay is 0 sec
  RXload is 1 ,Txload is 1
  Tunnel source 2.2.2.1 (FastEthernet 1/1), destination 1.1.1.1
  Tunnel protocol/transport GRE/IP, key 0x12d687, sequencing disabled
  Checksumming of packets disabled  Queueing strategy: WFQ
  5 minutes input rate 11 bits/sec, 0 packets/sec
  5 minutes output rate 11 bits/sec, 0 packets/sec
    85 packets input, 4452 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    65 packets output, 3496 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
```

R2# show ip route

```
Codes: C- connected, S- static,  R- RIP
       O- OSPF, IA- OSPF inter area
       N1- OSPF NSSA external type 1, N2- OSPF NSSA external type 2
       E1- OSPF external type 1, E2- OSPF external type 2
       * - candidate default

Gateway of last resort is 2.2.2.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 2.2.2.2
C     2.2.2.0/30 is directly connected, FastEthernet 1/1
C     2.2.2.1/32 is local host.
C     10.1.1.0/24 is directly connected, Tunnel 1
C     10.1.1.2/32 is local host.
R     192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:15, Tunnel 1
C     192.168.2.0/24 is directly connected, FastEthernet 1/0
C     192.168.2.1/32 is local host.
```

第十五步：验证测试。

（1）查看 R1 的 IKE SA，可以看到 IKE SA 协商成功，状态为 QM_IDLE。

```
R1# show crypto isakmp sa
destination    source       state          conn- id          lifetime(second)
2.2.2.1     1.1.1.1          QM_IDLE           33                  84170
e3e0dddad7d4d1ce   0e6cc92784e23f9d
```

（2）查看 R1 的 IPSec SA，可以看到两个 IPSec SA 协商成功，一个用于入站报文，一

个用于出站报文。

```
R1# show crypto ipsec sa

Interface: FastEthernet 1/0
          Crypto map tag:to_r2, local addr 1.1.1.1
          media mtu 1500
          ==================================================
          item type:static, seqno:1, id=32
          local   ident (addr/mask/prot/port): (1.1.1.1/0.0.0.0/47/0)
          remote   ident (addr/mask/prot/port): (2.2.2.1/0.0.0.0/47/0)
          PERMIT
          #pkts encaps: 81, #pkts encrypt: 81, #pkts digest 81
          #pkts decaps: 61, #pkts decrypt: 61, #pkts verify 61
          #send errors 0, #recv errors 0

          Inbound esp sas:
                spi:0x6e729d63 (1853005155)
                transform: esp-3des esp-sha-hmac
                in use settings={Transport,}                    !传输模式
                crypto map to_r2 1
                sa timing: remaining key lifetime (k/sec): (4606986/1315)
                IV size: 8 bytes
                Replay detection support:Y

           Outbound esp sas:
                spi:0x2ebb461 (49001569)
                transform: esp-3des esp-sha-hmac
                in use settings={Transport,}                    !传输模式
                crypto map to_r2 1
                sa timing: remaining key lifetime (k/sec): (4606986/1315)
                IV size: 8 bytes
                Replay detection support:Y
```

(3) 查看 R2 的 IKE SA,可以看到 IKE SA 协商成功,状态为 QM_IDLE。

```
R2# show crypto isakmp sa
  destination       source      state       conn-id        lifetime(second)
  2.2.2.1          1.1.1.1     QM_IDLE         33                83798
  e3e0dddad7d4d1ce  0e6cc92784e23f9d
```

(4) 查看 R2 的 IPSec SA,可以看到两个 IPSec SA 协商成功,一个用于入站报文,一个用于出站报文。

```
R2# show crypto ipsec sa
```

```
Interface: FastEthernet 1/1
        Crypto map tag:to_r1, local addr 2.2.2.1
        media mtu 1500
        ==================================================
        item type:static, seqno:1, id=32
        local   ident(addr/mask/prot/port): (2.2.2.1/0.0.0.0/47/0)
        remote   ident(addr/mask/prot/port): (1.1.1.1/0.0.0.0/47/0)
        PERMIT
        #pkts encaps: 75, #pkts encrypt: 75, #pkts digest 75
        #pkts decaps: 95, #pkts decrypt: 95, #pkts verify 95
        #send errors 0, #recv errors 0

        Inbound esp sas:
             spi:0x2ebb461(49001569)
             transform: esp-3des esp-sha-hmac
             in use settings={Transport,}                    !传输模式
             crypto map to_r1 1
             sa timing: remaining key lifetime (k/sec): (4607984/896)
             IV size: 8 bytes
             Replay detection support:Y

          Outbound esp sas:
             spi:0x6e729d63(1853005155)
             transform: esp-3des esp-sha-hmac
             in use settings={Transport,}                    !传输模式
             crypto map to_r1 1
             sa timing: remaining key lifetime(k/sec): (4607984/896)
             IV size: 8 bytes
             Replay detection support:Y
```

通过以上状态信息可以看出，R1 与 R2 成功协商了一个 IKE SA 和两个 IPSec SA（每个方向各一个）。

【注意事项】

- GRE 隧道两端的密钥要一致。
- 隧道两端的源和目的相互对应，即 R1 的源地址为 R2 的目的地址，R2 的源地址为 R1 的目的地址。
- 需要在 Tunnel 接口启用路由，而非连接 Internet 的接口。
- 确保 IPSec 隧道两端之间的连通性正常。
- 双方的 IKE 策略和 IPSec 转换集要一致，且双方的预共享密钥要一致。
- 当配置了多个 IKE 策略和 IPSec 转换集时，请确保双方能够协商出一个相同的策略和转换集。
- 双方的加密访问列表要互为镜像。

【参考配置】

R1# show running-config

```
Building configuration…
Current configuration : 1268 bytes
!
hostname R1
!
access-list 100 permit 47 host 1.1.1.1 host 2.2.2.1
!
no service password-encryption
!
crypto isakmp policy 1
  encryption 3des
  authentication pre-share
  hash sha
  group 2
!
crypto isakmp key 7 076f517c41477152 address 2.2.2.1
crypto ipsec transform-set 3des_sha  esp-3des esp-sha-hmac
  mode transport
crypto map to_r2 1 ipsec-isakmp
  set peer 2.2.2.1
  set transform-set 3des_sha
  match address 100
!
interface serial 1/2
  clock rate 64000
!
interface serial 1/3
  clock rate 64000
!
interface FastEthernet 1/0
ip address 1.1.1.1 255.255.255.252
  crypto map to_r2
  duplex auto
  speed auto
!
interface FastEthernet 1/1
ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
```

```
interface Tunnel 1
  no ip route-cache
  no ip route-cache policy
  ip address 10.1.1.1 255.255.255.0
  tunnel source FastEthernet 1/0
  tunnel destination 2.2.2.1
  tunnel key 1234567
  no keepalive
!
interface Null 0
!
router rip
  no auto-summary
  version 2
  network 10.0.0.0
  network 192.168.1.0
!
ip route 0.0.0.0 0.0.0.0 1.1.1.2
!
line con 0
line aux 0
line vty 0 4
  login
!
end
```

R2# show running-config

```
Building configuration…
Current configuration : 1268 bytes
!
hostname R2
!
access-list 100 permit 47 host 2.2.2.1 host 1.1.1.1
!
no service password-encryption
!
crypto isakmp policy 1
  encryption 3des
  authentication pre-share
  hash sha
  group 2
!
crypto isakmp key 7 076f517c41477152 address 1.1.1.1
```

```
crypto ipsec transform-set 3des_sha  esp-3des esp-sha-hmac
  mode transport
crypto map to_r1 1 ipsec-isakmp
  set peer 1.1.1.1
  set transform-set 3des_sha
  match address 100
!
interface serial 1/2
  clock rate 64000
!
interface serial 1/3
  clock rate 64000
!
interface FastEthernet 1/0
ip address 192.168.2.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet 1/1
ip address 2.2.2.1 255.255.255.252
  crypto map to_r1
  duplex auto
  speed auto
!
interface Tunnel 1
  no ip route-cache
  no ip route-cache policy
  ip address 10.1.1.2 255.255.255.0
  tunnel source FastEthernet 1/1
  tunnel destination 1.1.1.1
  tunnel key 1234567
  no keepalive
!
interface Null 0
!
router rip
  no auto-summary
  version 2
  network 10.0.0.0
  network 192.168.2.0
!
ip route 0.0.0.0 0.0.0.0 2.2.2.2
!
line con 0
```

```
line aux 0
line vty 0 4
  login
!
end
```

R3# show running-config

```
Building configuration…
Current configuration : 489 bytes
hostname R3
!
no service password-encryption
!
interface serial 1/2
  clock rate 64000
!
interface serial 1/3
  clock rate 64000
!
interface FastEthernet 1/0
  ip address 1.1.1.2 255.255.255.252
  duplex auto
  speed auto
!
interface FastEthernet 1/1
  ip address 2.2.2.2 255.255.255.252
  duplex auto
  speed auto
!
interface Null 0
!
line con 0
line aux 0
line vty 0 4
  login
!
!
end
```

第 2 章 VPN 专用设备远程访问安全

2.1 构建远程访问 IPSec VPN(用户口令)

【实验名称】

构建远程访问 IPSec VPN(用户口令)。

【实验目的】

学习配置远程访问 IPSec VPN 隧道,熟悉远程接入方式下的 VPN 隧道建立过程。

【背景描述】

某员工正在外地出差,由于需要查找资料,需要访问公司内部的服务器资源,而这些服务器资源因安全性考虑,并不直接在 Internet 公网上开放。因此该员工必须通过先和公司建立 VPN 隧道,才能获得访问公司内部资源的权力,实现公司保密数据在 Internet 上安全通信。

【需求分析】

需求:解决出差员工和公司之间通过 Internet 进行数据传输的安全问题。

分析:IPSec VPN 技术通过隧道技术、加解密技术、密钥管理技术、认证技术等有效地保证了数据在 Internet 中传输的安全性,是目前最安全、使用最广泛的 VPN 技术。可以通过建立远程访问的 IPSec VPN 加密隧道,实现出差员工和公司网络之间安全的数据传输。

【实验拓扑】

如图 2-1 所示的网络拓扑,是某公司员工在外地出差,需要访问公司内部的服务器资源,通过 Internet 网访问公司内网的工作场景。由于通过 Internet 数据传输的安全问题,公司服务器资源因安全性考虑不直接在公网上开放。外地用户远程访问公司内网中的各

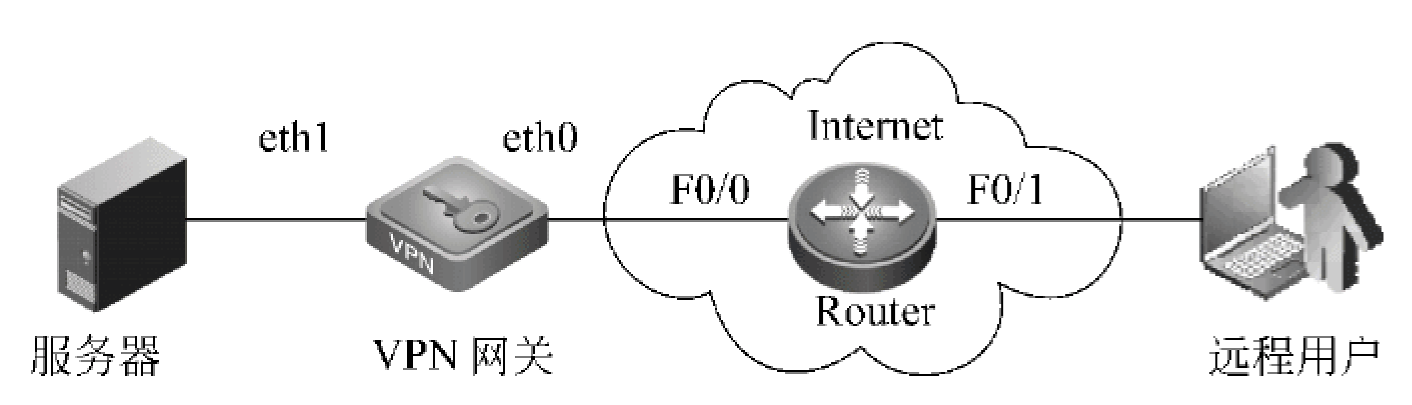


图 2-1 构建远程访问 IPSec VPN 用户口令网络拓扑

种网络资源，在 Internet 上传输数据，公司希望建立 IPSec VPN 加密隧道，构建远程访问 IPSec VPN 用户口令，员工通过公司提供的用户口令，通过 IPSec VPN 隧道获得访问公司内部资源，实现和公司网络服务器之间安全的数据传输。

【实验设备】

RG-WALL VPN 网关：1 台；RG-SRA 安全远程接入系统软件：1 套；路由器：1 台；PC：2 台（1 台作为公司内部服务器，1 台作为远程接入用户并安装 SRA 软件）。

【预备知识】

VPN 隧道技术

目前 VPN 主要采用四项技术来保证 VPN 通信安全，这四项技术分别是隧道技术、加解密技术、密钥管理技术、使用者与设备身份认证技术。

VPN 的隧道指的是利用一种网络协议来传输另一种网络协议的通信过程，它主要利用网络隧道协议来实现这种功能。网络隧道技术涉及了三种网络协议，即网络隧道协议、隧道协议下面的承载协议和隧道协议所承载的被承载协议。

网络隧道是指在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道技术是一种通过公共网络的基础设施，在专用网络或专用设备之间，实现加密数据通信的技术，隧道中的通信内容可以是任何通信协议的数据包。隧道协议将这些协议的数据包重新封装在新的包中发送，新的包头提供了路由信息，从而使封装的数据能够通过公共网络传递，传递时所经过的逻辑路径称为隧道。当数据包到达通信终点后，将被拆封并转发到最终目的地。隧道技术是指包括数据封装、传输和数据拆封在内的全过程。

VPN 隧道所使用公共网络可以是任何类型通信网络，可以是 Internet，也可以是企业内部网。为创建隧道 VPN 客户机和服务器必须使用相同隧道协议，常用隧道协议包括：点对点隧道协议 PPTP，第二层隧道协议 L2TP 和第三层隧道模式 IPSec。

按照开放系统互联 OSI 参考模型划分，隧道技术可以分为以第二层隧道协议为基础技术和以第三层隧道协议为基础技术。第二层隧道协议对应 OSI 模型中数据链路层，使用帧作为数据传输单位，PPTP 和 L2TP 协议属于第二层隧道协议，都是将数据封装在点对点协议（PPP）的帧中通过 Internet 发送。第三层隧道协议对应 OSI 模型中的网络层，使用包作为数据传输单位。IPSec 协议属于第三层隧道协议，是将数据包封装在附加了 IP 包头的新数据包中通过 IP 网络传送。

第二层隧道和第三层隧道的本质区别在于：用户的数据包是被封装在哪一层的数据包隧道里传输的。第二层隧道协议和第三层隧道协议分别使用，承担各自所在层的安全功能。合理地运用这两层隧道协议，将为网络提供更好的安全性。例如，L2TP 与 IPSec 协议的配合使用，可以分别形成 L2TP VPN、IPSec VPN 网络，也可混合使用 L2TP 和 IPSec 协议，形成性能更强大的 L2TP VPN 网络，且这一 VPN 网络形式是目前性能最好、应用最广的一种安全虚拟网，能提供更加安全的数据通信，解决了用户的后顾之忧。

点对点隧道协议（Point-to-Point Tunneling Protocol，PPTP）将使用点对点协议

(Point-to-Point Protocol,PPP)的封装 IP 数据包,通过 TCP/IP 网络进行传输。PPTP 可以对 IP、IPX 或 NetBEUI 数据包进行加密传递,通过 PPTP 控制连接来创建、维护和终止一条隧道,并使用通用路由封装对 PPP 数据帧进行封装。封装前,PPP 数据帧的有效载荷(有效传输数据)首先必须经过加密、压缩或是两者的混合处理。

第二层隧道协议(Layer Two Tunneling Protocol,L2TP)是 PPTP 和第二层转发技术(Layer Two Forward,L2F)的结合。第二层转发技术 L2F 是 Cisco 公司提出的隧道技术,为了避免 PPTP 和 L2F 两种互不兼容的隧道技术,在市场上彼此竞争给用户带来不便,Internet 工程任务委员会 IETF 要求将两种技术结合在单一隧道协议中,并在该协议中综合 PPTP 和 L2F 两者优点,由此产生了 L2TP。L2TP 协议将 PPP 数据帧封装后,可通过 TCP/IP、X.25、帧中继或 ATM 等网络进行传送,L2TP 可以对 IP、IPX 或 NetBEUI 数据进行加密传递。目前,IETF 组织仅定义了基于 TCP/IP 网络的 L2TP。

为了实现在专用或公共 IP 网络上的安全传输数据,安全 IP 隧道模式 IPSec 协议使用安全方式封装和加密整个 IP 包。它首先对 IP 数据包进行加密,然后将密文数据包再次封装在明文 IP 包内,通过网络发送到接收端的 VPN 设备。VPN 设备对收到的数据包进行处理,再去除明文 IP 包头,对内容进行解密之后,获得原始的 IP 数据包,再根据其路由信息把数据转发到目标网络的接收计算机。

在这三种隧道协议中,点对点隧道协议 PPTP 和第二层隧道协议 L2TP 的优点是:对使用微软公司操作系统的用户来说很方便,因为微软公司已把它们作为路由软件的一部分;缺点是 PPTP 和 L2TP 将不安全的 IP 数据包封装在安全的 IP 数据包内。PPTP 和 L2TP 适用于远程访问虚拟专用网。安全 IP 隧道模式 IPSec 的优点是它定义了一套用于认证、保护私密和数据完整性的标准协议,缺点是微软公司对 IPSec 的支持不够。IPSec 适用于可信的局域网之间的虚拟专用网,即企业内部网 VPN 应用。

【实验原理】

IPSec 协议的主要作用是为 IP 数据通信提供安全服务。IPSec 不是一个单独协议,它是一套完整的体系框架,包括 AH、ESP 和 IKE 三个协议。IPSec 使用了多种加密算法、散列算法、密钥交换方法等为 IP 数据流提供安全性,它可以提供数据的机密性、数据的完整性、数据源认证和反重放等安全服务。

使用 IPSec 可以构建两种不同接入方式的 VPN,即远程访问 VPN 和站点到站点 VPN,本实验中使用 IPSec 来构建远程访问 VPN。

远程用户 PC 与公司 VPN 网关通过 IKE 自动协商建立起远程访问 IPSec VPN 加密隧道,使得远程用户 PC 能安全地访问到 VPN 网关所保护的内部服务器。

远程用户 PC 在和 VPN 网关建立 VPN 隧道前,需要先获得 VPN 网关的身份验证许可。该实验所采用的用户身份验证为口令方式。

远程用户 PC 在通过 VPN 网关的身份验证后,VPN 网关会自动将 VPN 隧道建立(即 IKE 协商)所需要的配置下发给远程用户 PC,然后远程用户 PC 与 VPN 网关之间自动开始 IKE 协商,协商成功后 VPN 隧道即建立成功。整个过程系统自动完成,无须人为干预,是免配置的典型方式。

【实验步骤】

第一步：准备好 PC 和服务器。

在远程用户 PC 上安装 SRA 远程接入软件，安装完成后可能需要重新启动 PC。

在服务器 PC 上安装 VPN 管理软件。

具体的安装过程不在这里进行详述，可以查看 VPN 产品的随机说品书和产品光盘。

第二步：搭建拓扑，配置 IP 地址。

按照如图 2-1 所示拓扑图，搭建实验拓扑，并根据如表 2-1 所示编址方案，配置各设备的 IP 地址。

表 2-1　设备 IP 地址

设　　备	接　　口	地　　址
VPN 网关	eth1 接口地址	192.168.2.1
	eth0 接口地址	10.1.1.1
PC	PC 的 IP 地址	10.1.2.1
	PC 网关地址	10.1.2.2
服务器	服务器的 IP 地址	192.168.2.2
	服务器网关地址	192.168.2.1
Router	F0/0 地址	10.1.1.2
	F0/1 地址	10.1.2.2

说明：PC 及 Router 地址的配置方式不再进行详述。

(1) 通过服务器的超级终端，在命令行下配置 VPN 网关的 eth1 口地址，操作如图 2-2 所示(注意：VPN 网关出厂时 eth1 口默认地址为 192.168.1.1/24)。

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manu
al):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.2.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# _
```

图 2-2　配置 VPN 网关的 eth1 口地址

(2) 通过服务器上 VPN 管理软件登录 VPN 网关，配置 eth0 口地址，操作如图 2-3 所示。

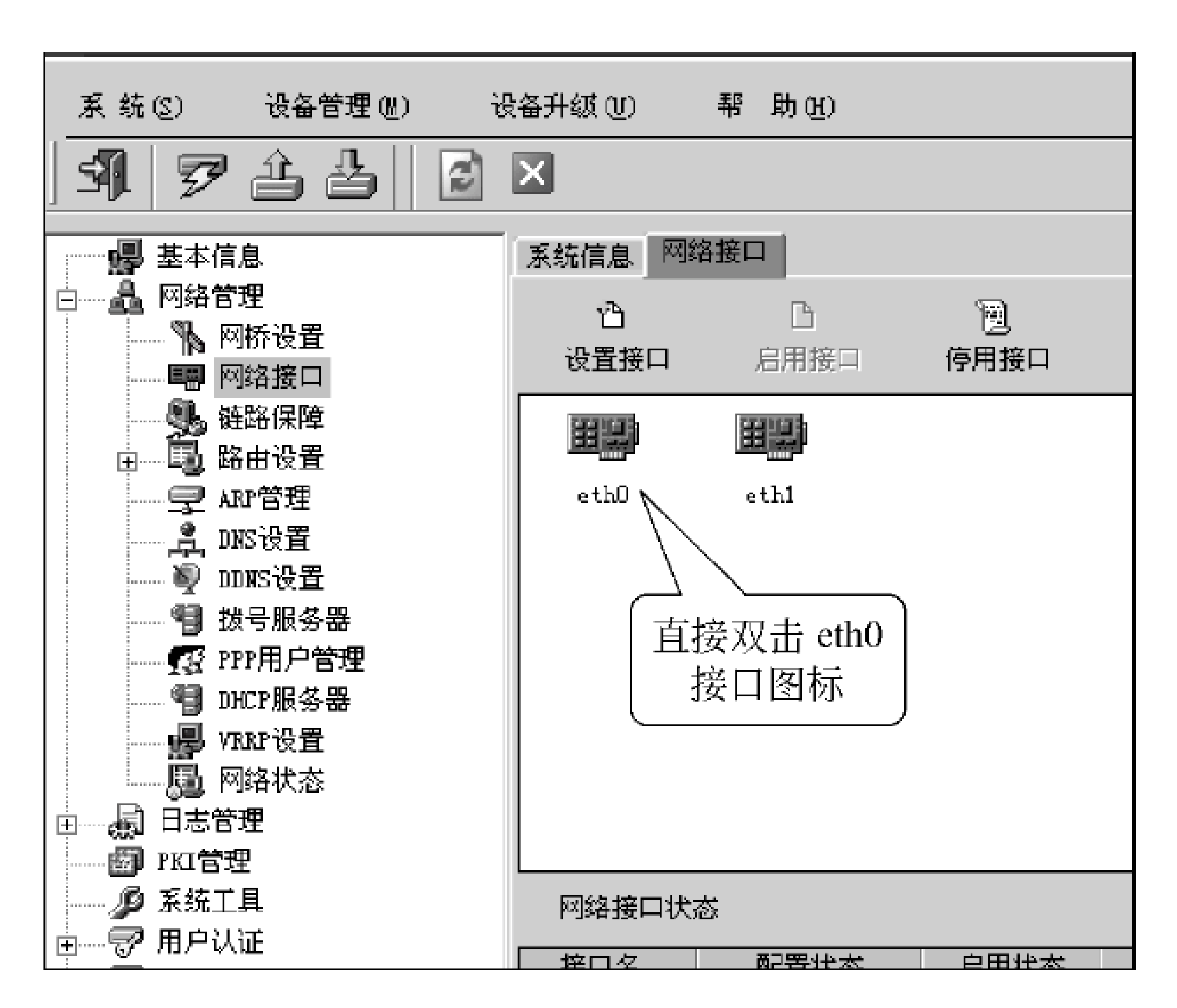


图 2-3 配置 eth0 口地址(1)

设置 eth0 接口地址,如图 2-4 所示。

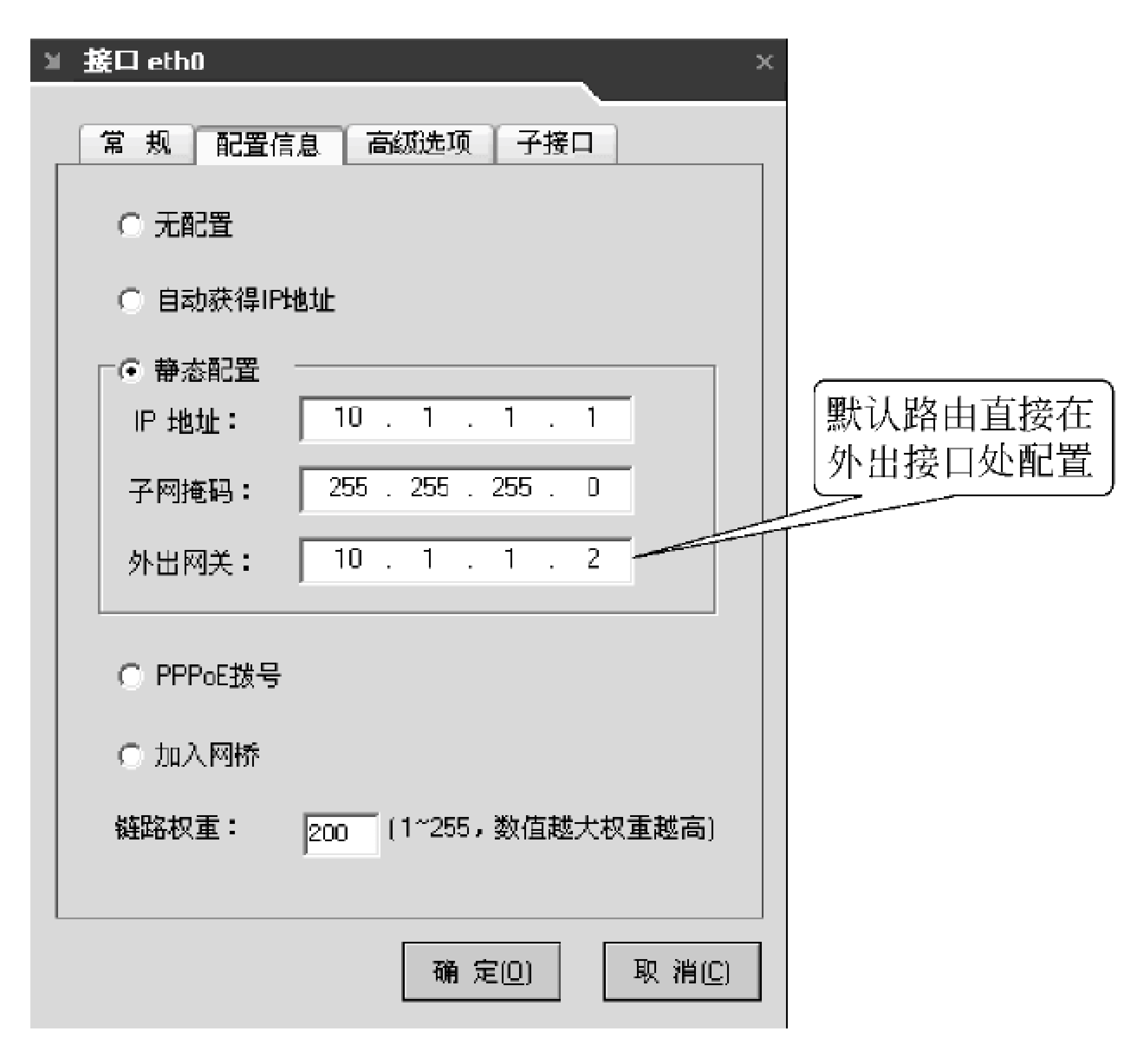


图 2-4 配置 eth0 口地址(2)

第三步:配置 IPSec VPN 隧道。

(1) 进入远程移动用户 VPN 隧道配置的界面。

登录 VPN 网关的管理界面,进入“远程用户管理”界面,如图 2-5 所示。

(2) 在图 2-5 所示“远程用户管理”界面上,选择“允许访问子网”项,打开配置“允许访问子网”信息,如图 2-6 所示,配置地址信息。

(3) 在图 2-5 所示“远程用户管理”界面上,选择“本地用户数据库”项,打开配置“本地用户数据库”信息, 如图 2-7 所示。



图 2-5　配置远程用户管理功能

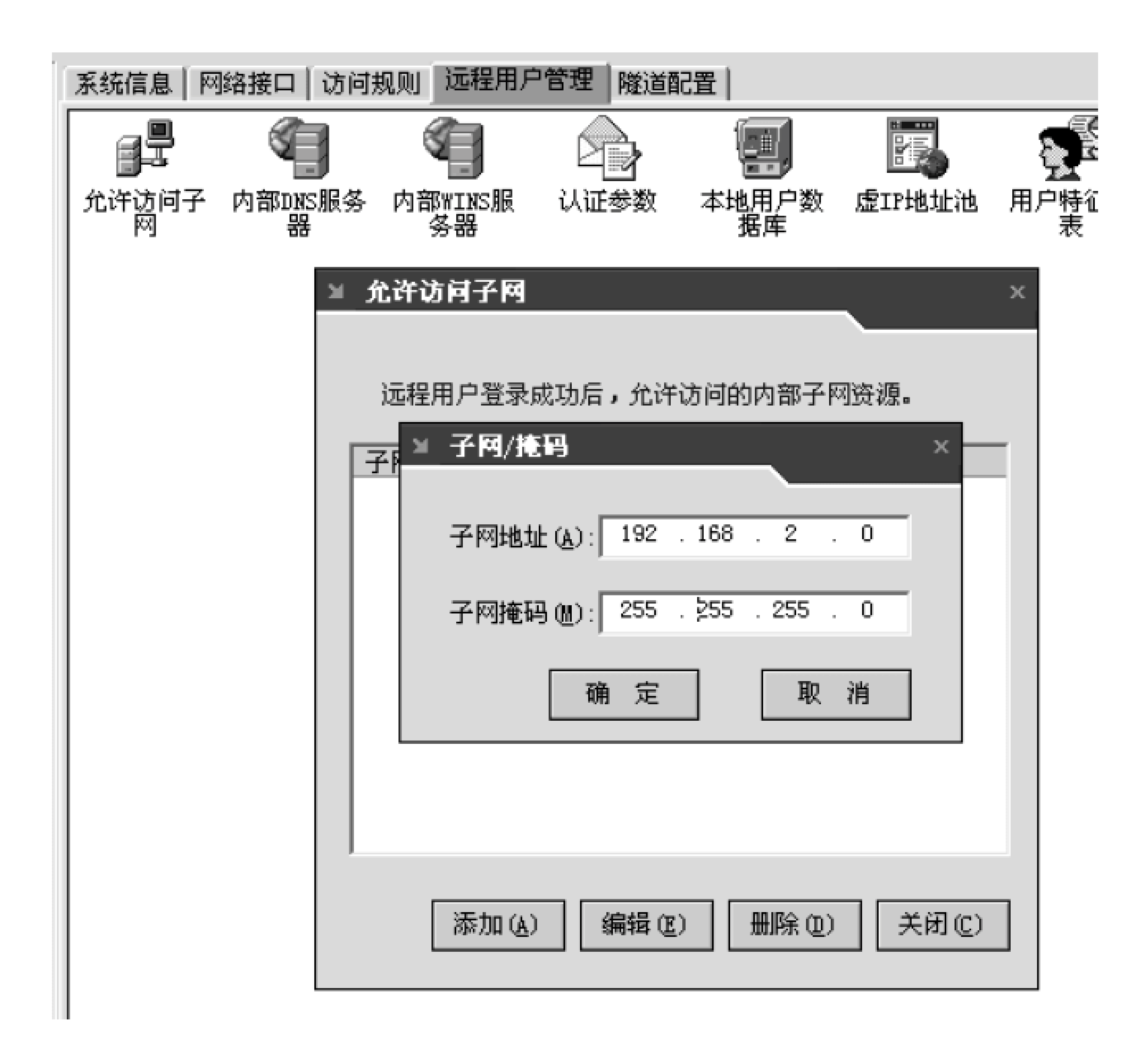


图 2-6　配置“允许访问子网”信息

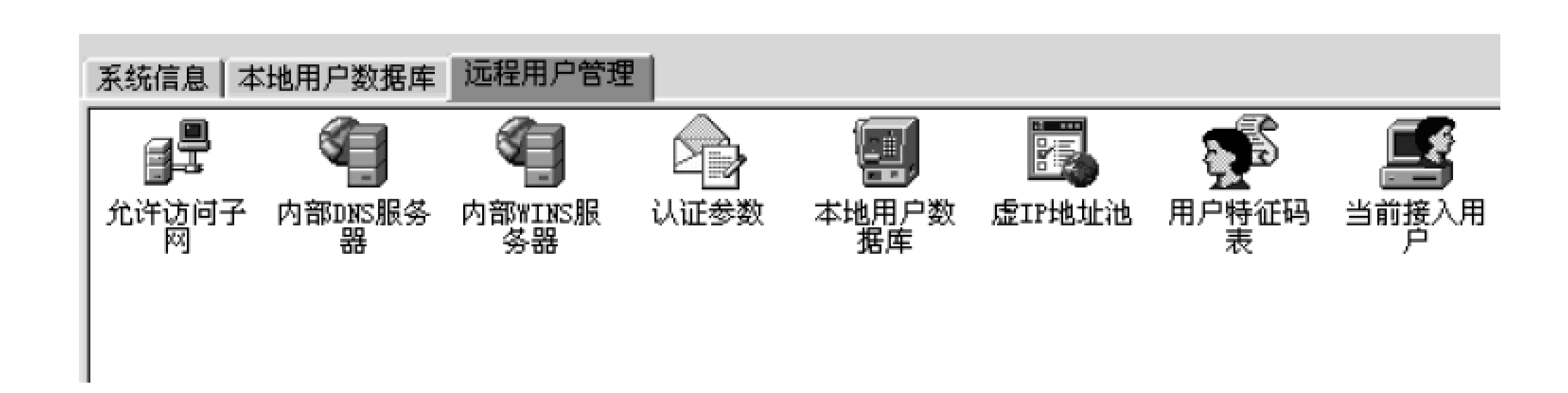


图 2-7　配置“本地用户数据库”信息

在打开的“本地用户数据库”配置信息界面上，选择“本地用户数据库”项，打开本地用户数据库，单击“添加用户”按钮，为设备添加远程访问的用户信息，包括用户名、口令和用户权限等，如图 2-8 所示。

在图 2-8 所示的“本地用户数据库”配置信息界面上，单击“用户生效”按钮，让配置的用户信息生效(注意：添加完用户后一定要单击“用户生效”按钮，否则新添加的用户依然

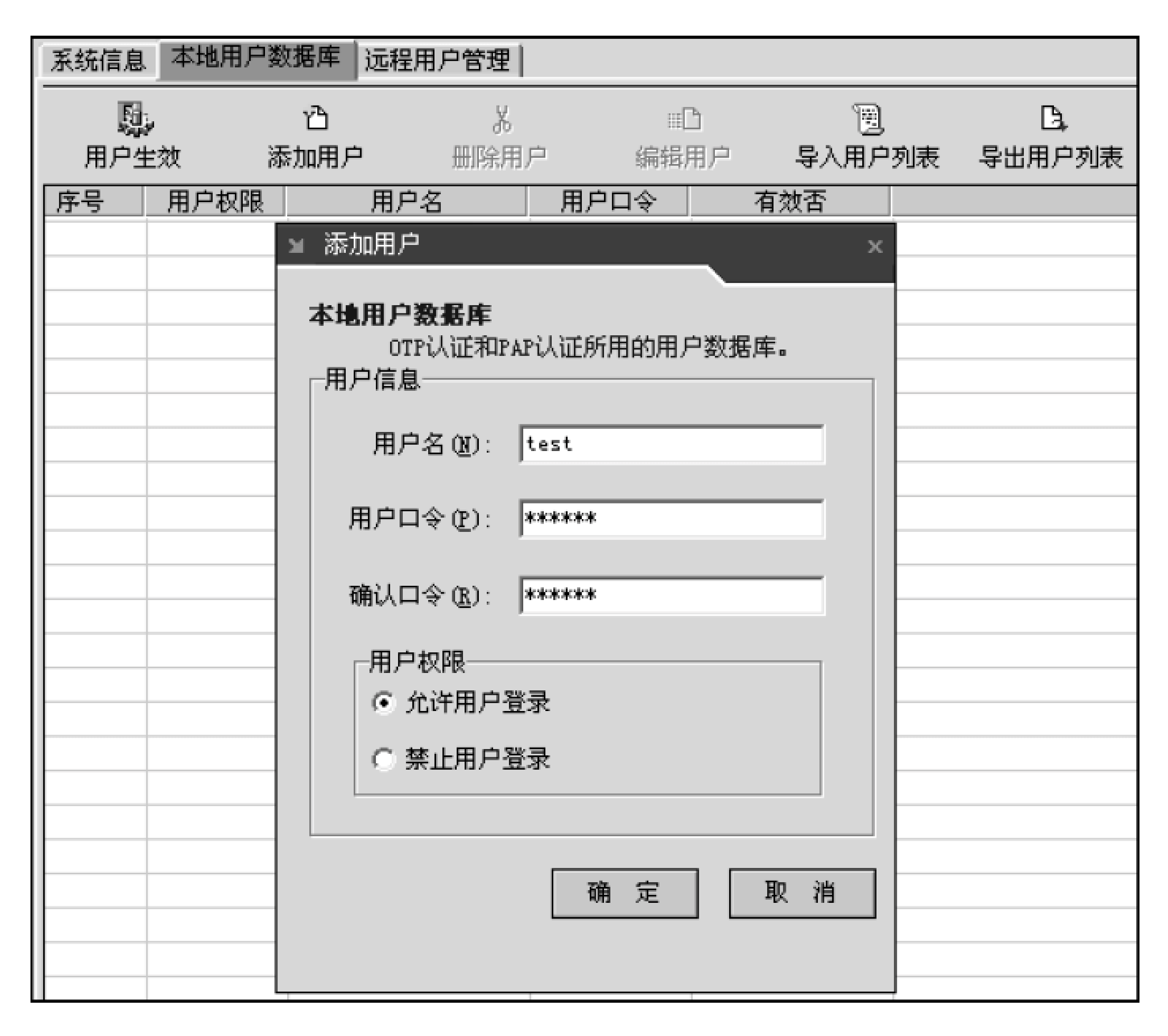


图 2-8 添加远程访问用户信息

不可使用),如图 2-9、图 2-10 所示。



图 2-9 让配置的用户信息生效(1)



图 2-10 让配置的用户信息生效(2)

(4) 配置“虚 IP 地址池”。

在图 2-7 所示的“远程用户管理”界面上,选择“虚 IP 地址池”图标,打开配置“虚 IP 地址池”信息,如图 2-11 所示。

在打开“虚 IP 地址池”管理界面上,选择“添加”、“删除”、“编辑”图标,配置“子网地

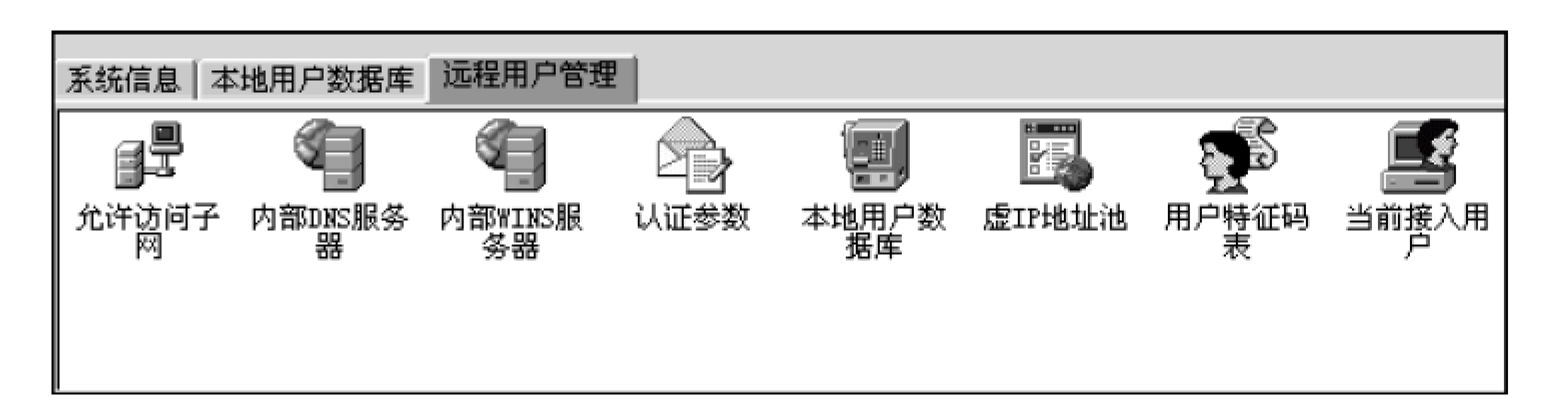


图 2-11　配置“虚 IP 地址池”信息(1)

址、连续地址”信息，如图 2-12 所示。



图 2-12　配置“虚 IP 地址池”信息(2)

注意：分配 PC 机的虚拟 IP 地址，既可以是定义一个地址池，由 VPN 网关自动分配；也可以是管理员一个 IP 对应一个用户的分配。本实验选择地址池方式，由系统自动分配，并且选择定义“子网地址”的地址池。

虚 IP 是网络管理员分配给远程移动用户的 IP，表示只有拥有该 IP 的 PC 机才能获得局域网内部的访问权限。因此，管理员设置的虚 IP 一定不要与远程 PC 的 IP 以及局域网内部的 IP 互相冲突，否则远程 PC 在和 VPN 网关建立隧道后，因地址冲突的问题，也无法访问局域网内部的服务器。本实验中虚 IP 地址池选择定义一个完全没有使用的网段。

如图 2-13 所示，在打开“虚 IP 地址池”管理界面上，选择“添加”图标，配置如图所示子网地址信息。

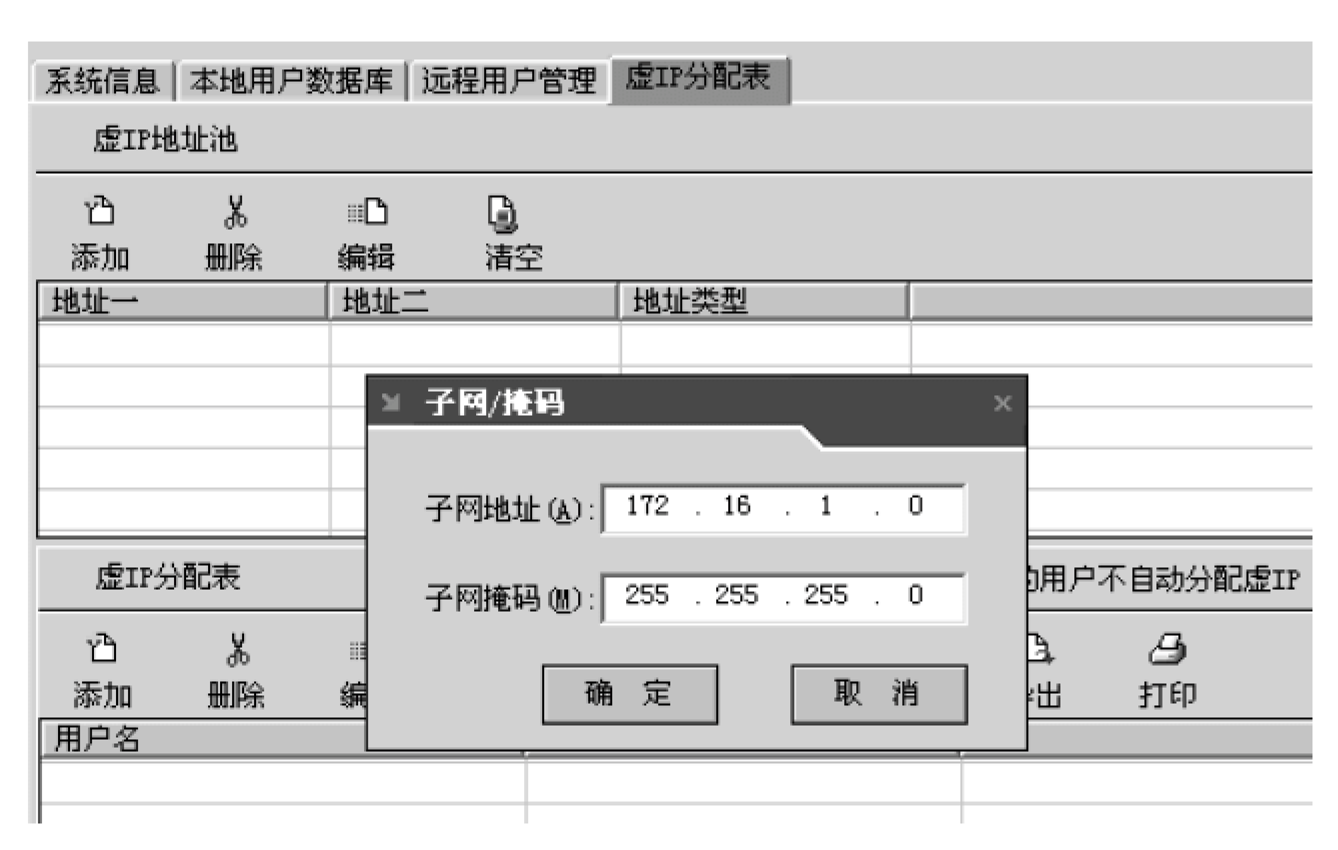


图 2-13　配置添加子网地址信息(1)

添加成功的子网地址信息,如图 2-14 所示。

系统信息 | 本地用户数据库 | 远程用户管理 | 虚IP分配表

虚IP地址池

添加 删除 编辑 清空

地址一	地址二	地址类型
172.16.1.0	255.255.255.0	子网地址

图 2-14　配置添加子网地址信息(2)

(5) 配置“用户特征码表”。

在如图 2-5 所示的“远程用户管理”界面上,选择“用户特征码表”图标,打开配置“用户特征码表”信息,如图 2-15 所示。

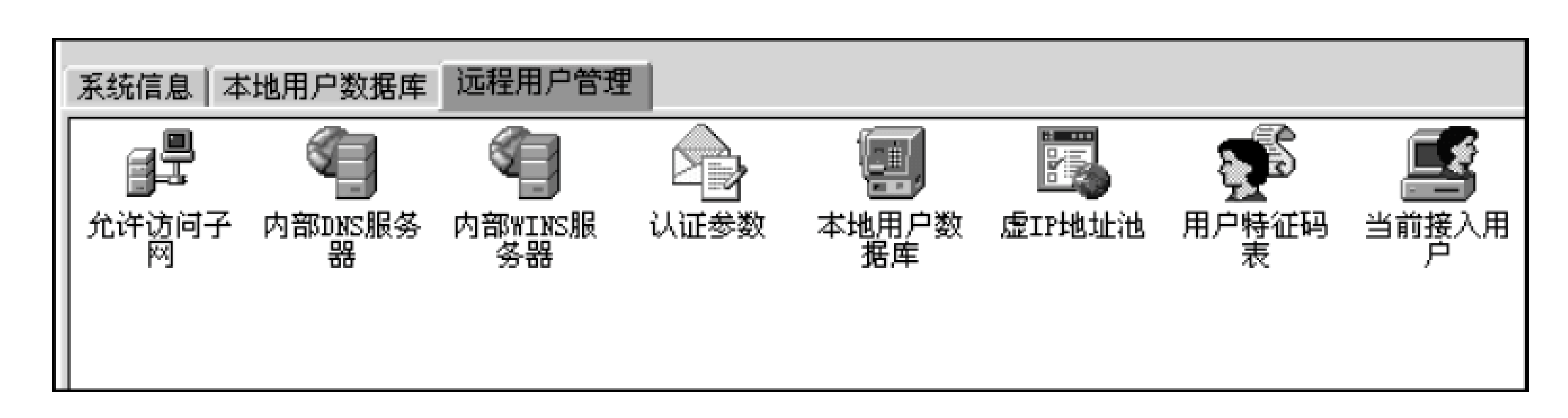


图 2-15　配置“用户特征码表”信息

打开“用户特征码表”图标后,选择“允许用户接入”策略,分配接入用户的接入权限:允许接入,如图 2-16 所示。

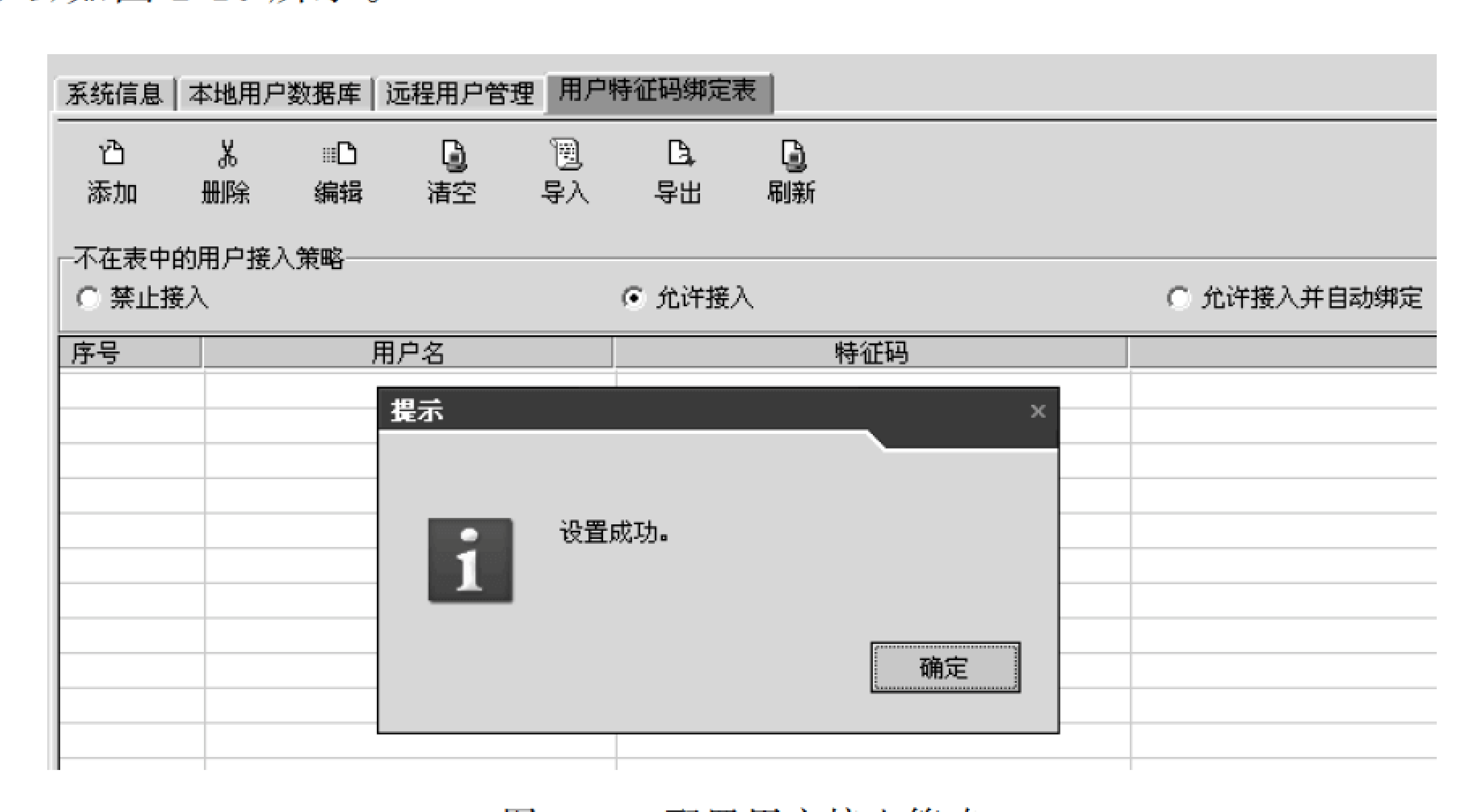


图 2-16　配置用户接入策略

配置说明:“用户特征码表”是为需要将远程 PC 的硬件和分配给用户的身份信息绑定的需求而设计的。选择了“允许接入并自动绑定”功能,则 VPN 网关会将远程用户的 PC 硬件特征码与该用户的身份认证信息相互绑定,绑定后该用户将无法用自己的身份信息再在其他 PC 设备上建立 VPN 隧道。

在实验中既可以选择“允许接入”,也可以选择“允许接入并自动绑定”。系统默认配

置是“禁止接入”。图示选择的是“允许接入”，这表示该用户的身份信息不会和其使用的 PC 硬件绑定。

此次实验，“远程用户管理”界面的其他配置项，例如，“内部 DNS 服务器”、“内部 WINS 服务器”、“认证参数”，用户可以根据实际需要选择设置。但该实验因为不涉及这些应用，故不需要进行设置。

第四步：配置远程接入客户端。

（1）第一次运行 RG-SRA 程序后，如图 2-17 所示。

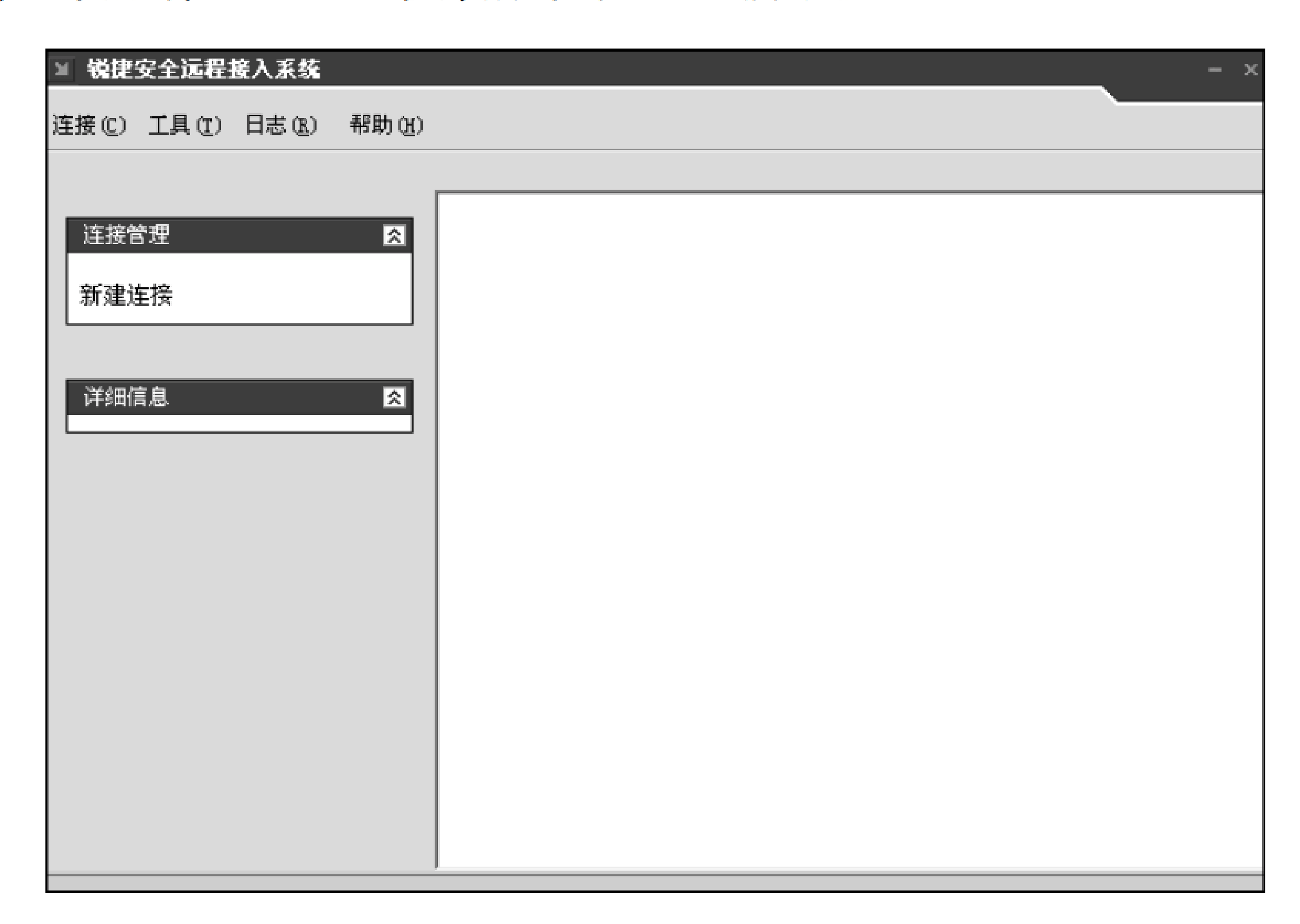


图 2-17　运行 RG-SRA 程序

（2）建立一个与 VPN 网关的隧道连接。

在运行 RG-SRA 程序主界面上，单击“新建连接”按钮，建立一个与 VPN 网关的隧道连接，如图 2-18 所示。



图 2-18　新建 VPN 网关的隧道连接

在新建 VPN 网关"添加新连接"的隧道连接上，填写新建 VPN 网关的隧道连接的基本信息：连接标识、服务器地址、认证方式等，如图 2-19 所示。



图 2-19 配置新建隧道连接的基本信息(1)

如图 2-20 所示是配置成功"添加新连接"基本信息。

单击"确定"按钮后，显示建立完成的一个"与 VPN 网关的隧道"连接标号，如图 2-21 所示。

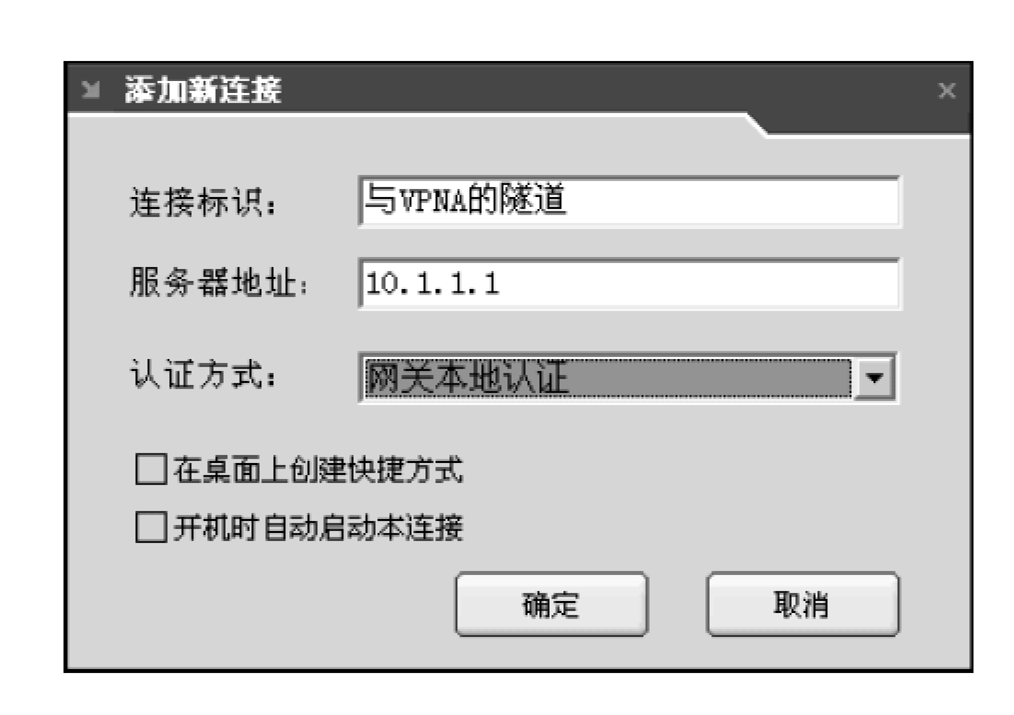


图 2-20 配置新建隧道连接的基本信息(2)



图 2-21 建立完成 VPN 网关的隧道连接

(3) 运行该隧道连接，建立 VPN 隧道。

在图 2-21 所示运行 RG-SRA 程序主界面上，单击"连接管理"按钮，选择新建立"与 VPN 网关的隧道"连接，右击打开快捷菜单，选择"启动连接"命令，启动新建的隧道连接，如图 2-22 所示。

选择快捷菜单中"启动连接"命令，启动新建的隧道连接，打开如图 2-23 所示的"连接 VPN"对话框，输入身份认证所必需的账号，即在图 2-8 所示对话框中 VPN 网关上添加的用户信息。

在图 2-23 对话框中输入身份认证信息后，单击"连接"按钮后，系统自动进行身份认证，并且开始 IKE 协商，如图 2-24 所示。系统自动进行身份认证后，与远程隧道连接建立

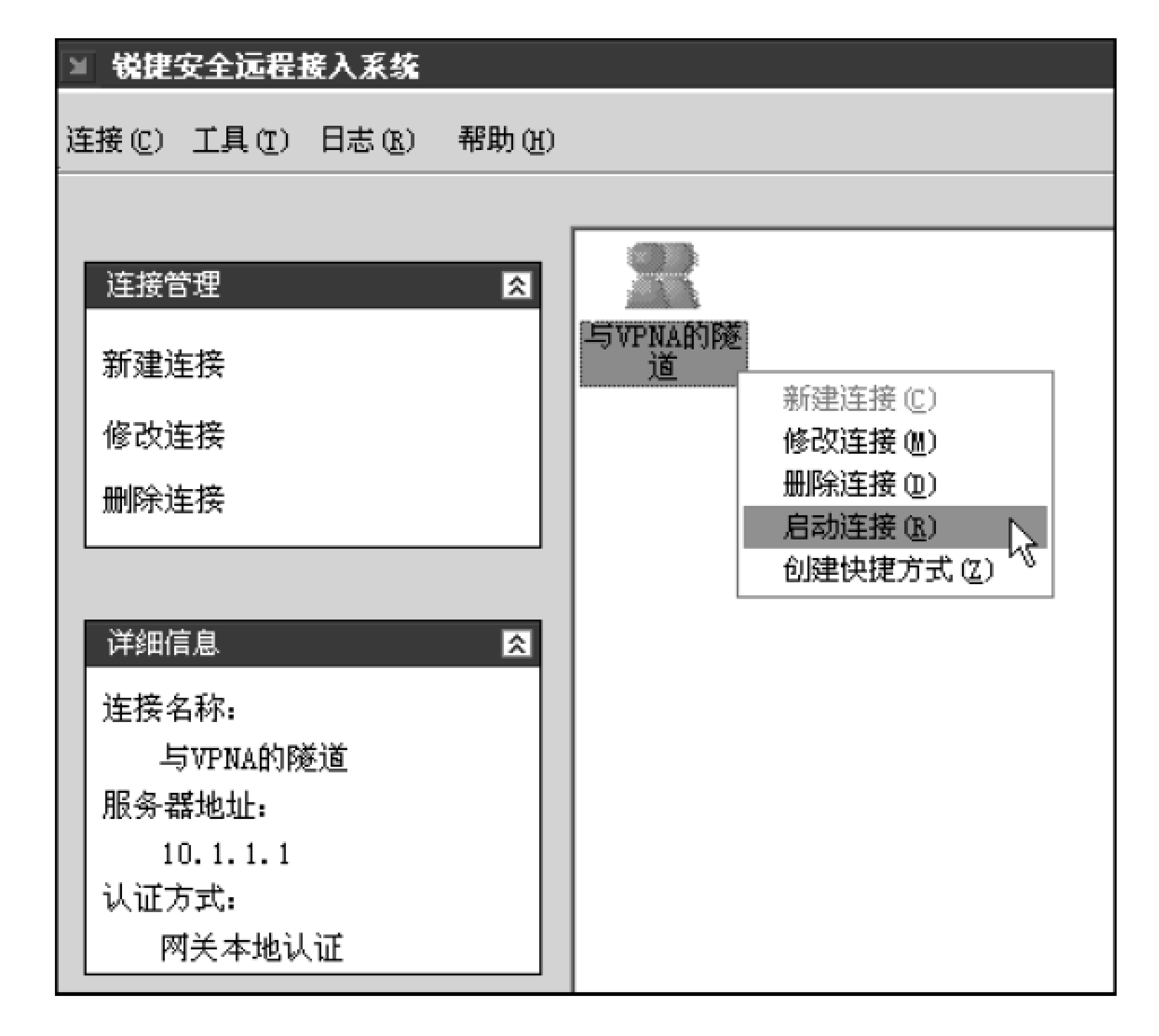


图 2-22　启动新建的隧道连接



图 2-23　登录 VPN 远程安全接入系统



图 2-24　系统自动进行身份认证

成功,SRA 程序会自动缩小图标显示在系统桌面屏幕的右下角,如图 2-25 所示。

选择 SRA 程序运行成功缩小图标,右击打开快捷菜单,在菜单中选择“详细配置”,可以查看到隧道信息,如图 2-26 所示。



图 2-25 SRA 程序运行成功缩小图标



图 2-26 查看到隧道信息

如图 2-27 所示信息为查看到隧道信息,显示“可访问”表示隧道已建立成功,如果是“不可访问”则表示隧道没有建立成功。“资源信息”中显示的“虚拟 IP 地址”信息,表示该 IP 为 VPN 网关从虚地址池中自动分配给该 PC 的虚 IP。

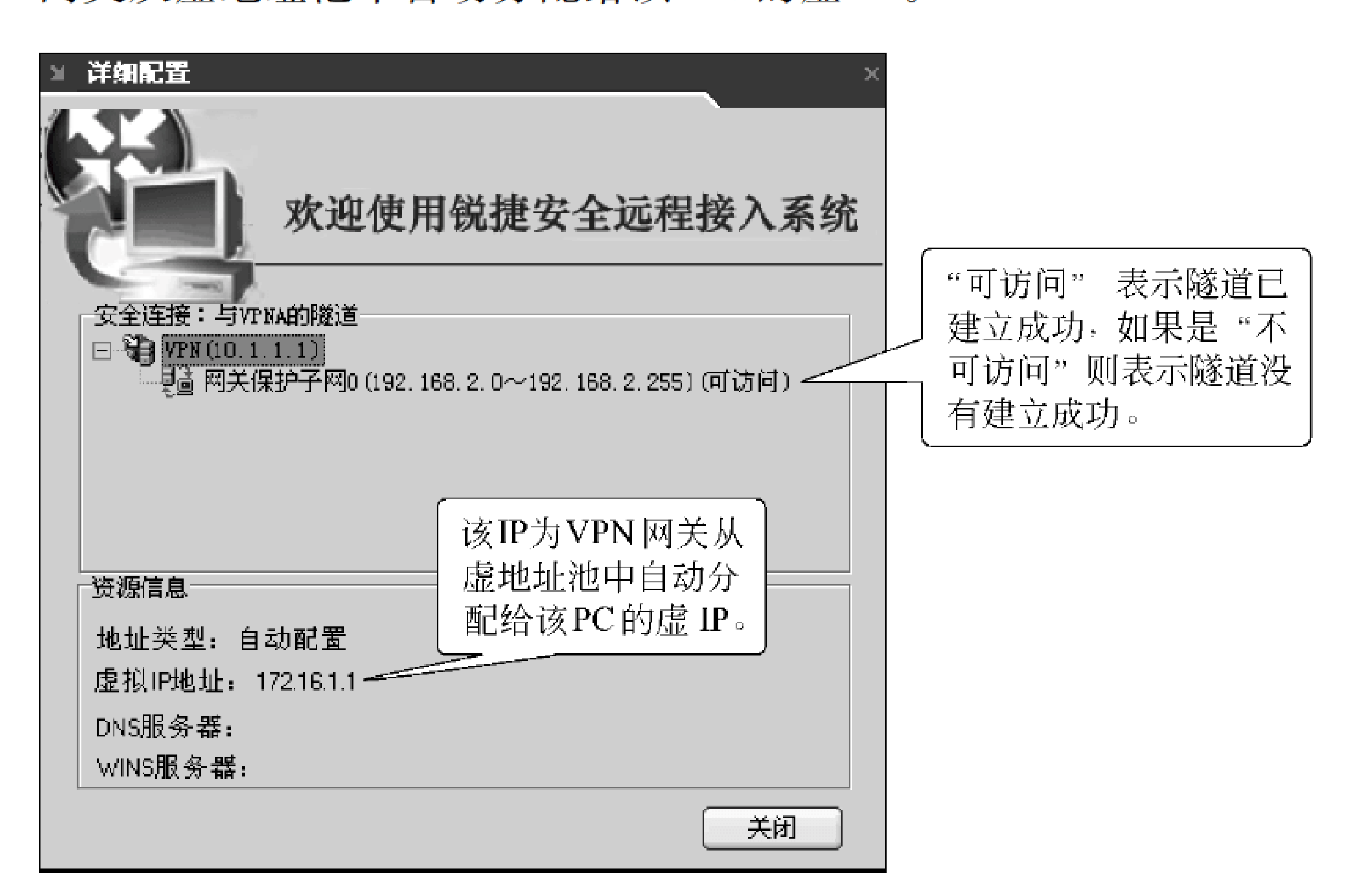


图 2-27 显示隧道配置信息内容

第五步:验证测试。

如图 2-28 所示信息,在图 2-5 所示 VPN 网关的管理界面,可看到已经建立成功的隧道信息,选择“隧道协商状态”项,可以查看隧道协商信息。

隧道启动后,可以在“隧道协商状态”栏目下,看到隧道的协商状态。打开后“隧道状态”显示“第二阶段协商成功”。VPN 隧道通信情况可以在“隧道协商状态”中查看到,如图 2-29 所示。

第六步:进行隧道通信。

在远程用户 PC 机上去访问服务器提供的服务可以

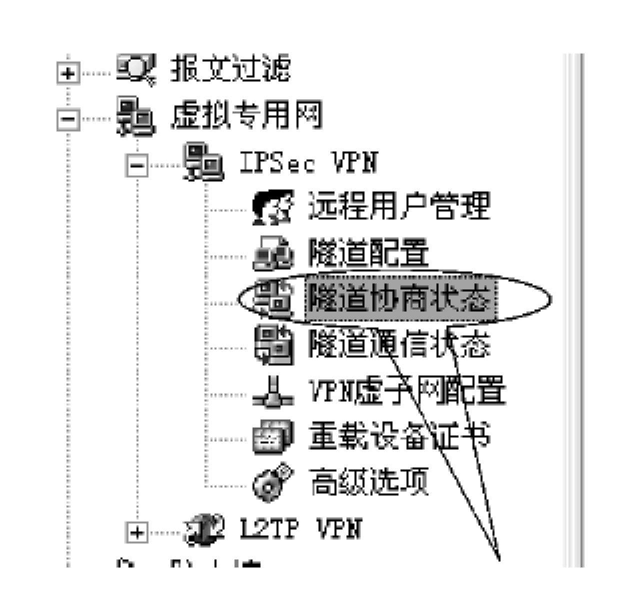


图 2-28 查看隧道协商信息(1)

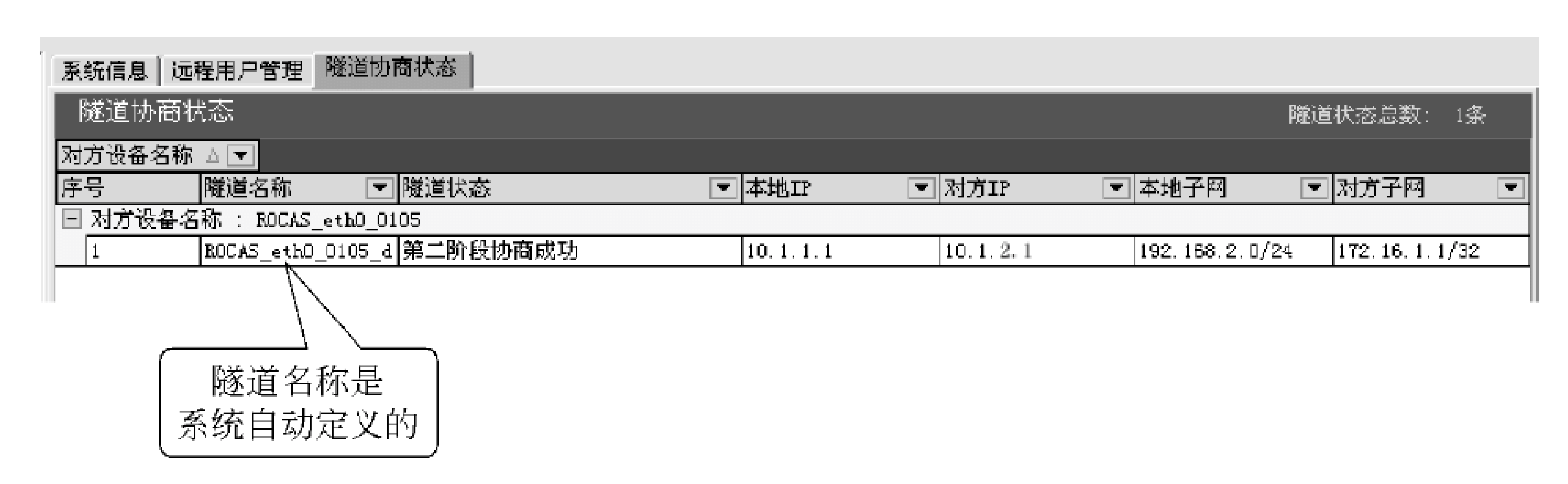


图 2-29　查看隧道协商信息(2)

成功，或者在 PC 上 ping 服务器的 IP 地址可以 ping 通(没有 VPN 隧道前 ping 会是失败的)。

如图 2-30 所示，在 VPN 网关的管理界面，选择“隧道通信状态”可以查看隧道通信信息。

隧道启动后，在“隧道通信状态”栏目下看到隧道通信状态，“隧道状态”显示“第二阶段协商成功”。VPN 隧道的通信情况可以在“隧道通信状态”中查看到，如图 2-31 所示。

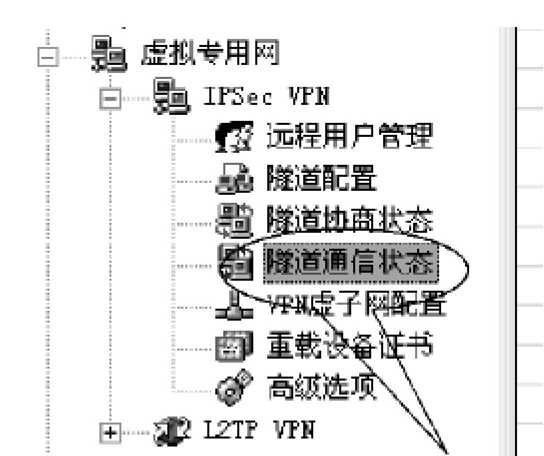


图 2-30　查看隧道通信信息(1)

系统信息 | 网络接口 | 隧道配置 | 隧道通信状态 | 隧道协商状态

隧道通信状态

序号	类型	本地子网	对方子网	发送成功包数	发送失败包数	发送成功字节数
1	IKE	192.168.2.0/24	192.168.1.0/24	14	0	840

隧道通信统计

校验失败包数	发生重播包数	非法加密包数
0	0	0

图 2-31　查看隧道通信信息(2)

【注意事项】

- 实验环境地址可以随意定义，但请不要使用 1.1.1.0 这个网段的 IP，因为某些功能实现的需要，VPN 系统内部已占用该网段的部分 IP。
- 该实验中，VPN 网关的防火墙规则为全部开放。但在实际的网络环境中，如果 VPN 网关直接连接 Internet 网络，则一定需要启用防火墙规则。
- RG-SRA 是 VPN 客户端软件程序，如果 PC 机上已预装其他厂家的 VPN 客户端程序，请先卸载其他厂家的 VPN 客户端程序，否则可能 RG-SRA 无法正常工作。

- RG-SRA 作为安全产品,安装后会对系统的网卡、端口、协议等方面有改动,因此会和部分防火墙或者防病毒程序不兼容。推荐用户使用没有安装任何第三方防火墙、防病毒程序的机器来做实验。

2.2 构建远程访问 IPSec VPN(USB-Key 数字证书)

【实验名称】

构建远程访问 IPSec VPN(USB-Key 数字证书)。

【实验目的】

学习配置远程访问(Remote Access)IPSec VPN 隧道,熟悉远程接入方式下的 VPN 隧道建立过程。同时掌握采用 USB Key 数字证书身份认证方式建立远程访问 VPN 技术。

【背景描述】

某员工正在外地出差,但需要访问公司内网中的服务器资源,而这些服务器资源因安全性考虑,并不直接在 Internet 公网上开放。因此该员工必须通过先和公司建立 VPN 隧道,获得访问内部资源的权力后才能访问公司内网中服务器资源。

远程接入用户在建立 VPN 隧道前,必须获得公司 VPN 网关的身份许可。为了更加安全需要,用户的身份信息保存,不采用传统的口令方式,而是采用 USB Key 设备的方式(USB Key 内存储标示用户身份的数字证书)。

【需求分析】

需求:解决出差员工和公司内网之间,通过 Internet 进行数据传输的安全问题。

分析:IPSec VPN 技术通过隧道技术、加解密技术、密钥管理技术、认证技术等有效地保证了数据在 Internet 中传输的安全性,是目前最安全、使用最广泛的 VPN 技术。可以通过建立远程访问的 IPSec VPN 加密隧道,实现出差员工和公司内网服务器之间安全的数据传输。

采用 USB Key 设备存储用户的数字证书,可以防止数字证书被盗用,这也是目前最为安全的一种身份认证方式。

【实验拓扑】

如图 2-32 所示网络拓扑,是某公司员工在外地出差,需要访问公司内网中的服务器资源。由于通过 Internet 数据传输的安全问题,公司服务器资源因安全性考虑不直接在公网上开放。外地远程访问总公司的各种网络资源,在 Internet 上传输数据,公司希望建

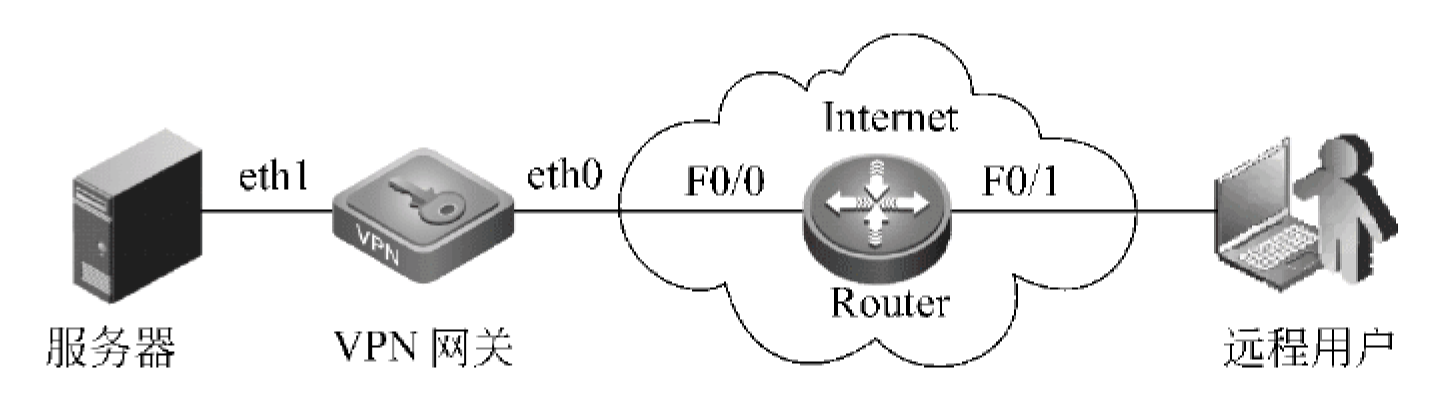


图 2-32　构建远程访问 IPSec VPN 网络拓扑

立 IPSec VPN 加密隧道。为了保障用户的身份信息安全，不采用传统的口令方式，而是采用 USB Key 设备的方式，通过 IPSec VPN 隧道获得访问内部资源，实现和总公司之间安全的数据传输。

【实验设备】

RG-WALL VPN 网关：1 台；RG-SRA 安全远程接入系统软件：1 套；RG-Key 密钥存储器：1 个；RG-CMS 证书管理系统软件：1 套；路由器：1 台；PC：2 台(1 台作为公司内部服务器，1 台作为远程接入用户并安装 SRA 软件)。

【预备知识】

IKE 工作原理

Internet Key Exchange，因特网密钥交换。它的作用是协助进行安全管理。IKE 在进行 IPSec 处理过程中，对身份进行鉴别，同时进行安全策略的协商，处理会话密钥的交换工作。Internet 密钥交换协议 IKE 主要用于 VPN 使用中加密密钥及提供分配密钥的一种方法，在 VPN 端点间，规定了如何保护数据的安全机制。

Internet 密钥交换(IKE)解决了在不安全的网络环境(如 Internet)中，安全地建立或更新共享密钥的问题。IKE 是非常通用的协议，不仅可为 IPSec 协商安全关联，而且可以为 SNMPv3、RIPv2、OSPFv2 等任何要求保密的协议协商安全参数。

IKE 属于一种混合型协议，由 Internet 安全关联、密钥管理协议(ISAKMP)和两种密钥交换协议 OAKLEY 与 SKEME 组成。IKE 主要有三项任务：为端点间的认证提供方法；建立新的 IPSec 连接(创建一对 SA)；管理现有连接。

IKE 跟踪连接的方法是给每个连接，分配一组安全联盟(SA)。SA 描述与特殊连接相关的所有参数，包括使用的 IPSec 协议(ESP/AH/二者兼有)，加密/解密和认证/确认传输数据使用的对话密钥。SA 本身是单向的，每个连接需要一个以上的 SA。大多数情况下，只使用 ESP 或 AH，每个连接要创建两个 SA，一个描述入站数据流，另一个描述出站数据流。同时使用 ESP 和 AH 的情况中就要创建 4 个 SA。

PKI/CA 数字证书

Internet 的发展和信息技术普及，给人们的工作和生活带来了前所未有的便利。然而，由于 Internet 所具有的广泛性和开放性，决定了 Internet 不可避免地存在着信息安全隐患。为了防范信息安全风险，许多新的安全技术和规范不断涌现，PKI(Public Key Infrastructure，公开密钥基础设施)即是其中一员。

PKI 产生于 20 世纪 80 年代，它是在公开密钥理论和技术基础上发展起来的一种综合安全平台，能够为所有网络应用透明地提供采用加密和数字签名等密码服务所必需的密钥和证书管理，从而达到保证网上传递信息的安全、真实、完整和不可抵赖的目的。为网络通信和网上交易提供身份认证，保证数据完整性、数据保密性、数据公正性、不可否认性及时间戳服务安全基础平台。

PKI 是一种遵循标准，它利用公钥加密技术为电子商务的开展，提供一套安全基础平台的技术和规范。PKI 的核心组成部分 CA(Certification Authority，认证中心)是数字证书的签发机构。数字证书，有时被称为数字身份证，是一个符合一定格式的电子文件，用

来识别电子证书持有者的真实身份。

利用 PKI 可以方便地建立和维护一个可信网络计算环境,从而使得人们在这个无法直接相互面对的环境里,能够确认彼此的身份和所交换的信息,能够安全地从事商务活动。

不难看出,建立以 PKI 为基础的安全解决方案,无论是对在 Intranet 上开展的无纸办公等内部业务,还是对电子支付、网上证券交易、网上购物、网上教育、网上娱乐等网络应用,都是一种安全可靠的选择。

PKI 安全的基础设施把公钥密码和对称密码结合起来,采用证书管理公钥。PKI 公钥基础同样遵循密码体制中,非对称密码体制的五个基本要素(公钥、私钥、原文、算法、密文)。密钥对应用数字证书保存、加密算法一般保存在证书当中,通过第三方的可信任机构:CA 认证中心保存。把用户的公钥和用户的其他标识信息捆绑在一起,在 Internet 网上验证用户的身份。

认证中心作为 PKI 的核心部分,CA 实现了 PKI 中一些很重要的功能,概括地说,认证中心的功能有证书发放、证书更新、证书撤销和证书验证。

CA 作为电子交易中受信任第三方,负责为电子商务环境中各个实体颁发数字证书,以证明各实体身份的真实性,并负责在交易中检验和管理证书。数字证书的用户拥有自己的公钥/私钥对。证书中包含有证书主体的身份信息、其公钥数据、发证机构名称等,发证机构验证证书主体为合法注册实体后,就对上述信息进行数字签名,形成证书。

在公钥证书体系中,如果某公钥用户需要任何其他已向 CA 注册的用户的公钥,可直接向该用户索取证书,而后用 CA 的公钥解密解密即可得到认证的公钥;由于证书中已有 CA 的签名来实现认证,攻击者不具有 CA 的签名密钥,很难伪造出合法的证书,从而实现了公钥的认证性。

数字证书认证中心是整个网上电子交易安全的关键环节,是电子交易中信赖的基础。它必须是所有合法注册用户所领带的具有权威性、依赖性及公正性的第三方机构。CA 的核心功能就是发放和管理数字证书。

概括地说,CA 的功能主要有证书发放、证书更新、证书撤销和证书验证。具体描述如下:

- 接收验证用户数字证书的申请。
- 确定是否接受用户数字证书的申请,即证书的审批。
- 向申请者颁发(或拒绝颁发)数字证书。
- 接收、处理用户的数字证书更新请求。
- 接收用户数字证书的查询、撤销。
- 产生和发布证书的有效期。
- 数字证书的归档。
- 密钥归档。
- 历史数据归档。

【实验原理】

IPSec 的主要作用是为 IP 数据通信提供安全服务。IPSec 不是一个单独协议,它是一套完整的体系框架,包括 AH、ESP 和 IKE 三个协议。IPSec 使用了多种加密算法、散

列算法、密钥交换方法等为 IP 数据流提供安全性，它可以提供数据的机密性、数据的完整性、数据源认证和反重放等安全服务。

远程用户 PC 与公司 VPN 网关通过因特网密钥交换协议 IKE，自动协商建立起远程访问 IPSec VPN 加密隧道，使得远程用户 PC 能安全地访问到 VPN 网关所保护的内部服务器。

远程用户 PC 在和 VPN 网关建立 VPN 隧道前，需要先获得 VPN 网关的身份验证许可，只有获得许可的用户，才可以安全地接入。本实验采用的用户身份验证为数字证书方式，数字证书由 CA 中心(即 RG-CMS 系统)颁发，并存储在 USB Key 设备(RG-Key)中。

远程用户 PC 在通过 VPN 网关的身份验证后，VPN 网关会自动将 VPN 隧道建立(即 IKE 协商)所需要的配置下发给远程用户 PC，然后远程用户 PC 与 VPN 网关之间自动开始 IKE 协商，协商成功后 VPN 隧道建立成功。整个过程系统自动完成，无需人为干预，是免配置的典型方式。

【实验步骤】

第一步：准备好 PC 机和服务器。

在远程用户 PC 上安装 SRA 远程接入软件，安装完成后需要重启 PC 方保证生效。

在服务器 PC 上安装 VPN 管理软件和 RG-CMS 系统。

另外，在安装 RG-CMS 和 RG-SRA 过程中，安装程序会提示要安装 USB Key(即 RG-Key)的驱动，请一定选择安装。

具体的安装过程不在这里进行详述，可以查看产品的随机说品书和产品光盘。

第二步：搭建拓扑，配置 IP 地址。

按照如图 2-32 所示拓扑图，搭建实验拓扑，并根据如表 2-2 所示编址方案，配置各设备的 IP 地址。

表 2-2　设备 IP 地址

设　　备	接　　口	地　　址
VPN 网关	eth1 接口地址	192.168.2.1
	eth0 接口地址	10.1.1.1
PC	PC 的 IP 地址	10.1.2.1
	PC 网关地址	10.1.2.2
服务器	服务器的 IP 地址	192.168.2.2
	服务器网关地址	192.168.2.1
Router	F0/0 地址	10.1.1.2
	F0/1 地址	10.1.2.2

说明：PC 及 Router 地址的配置方式不再详述。

(1) 通过服务器的超级终端，在命令行下配置 VPN 网关的 eth1 口地址，操作如图 2-33 所示(注意：VPN 网关出厂时 eth1 口默认地址为 192.168.1.1/24)。

(2) 通过服务器上 VPN 管理软件登录 VPN 网关，然后直接双击“eth0 接口”图标打开对话框，配置 eth0 口地址，操作如图 2-34 所示。

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manu
al):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.1.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# _
```

图 2-33　配置 VPN 网关 eth1 口地址

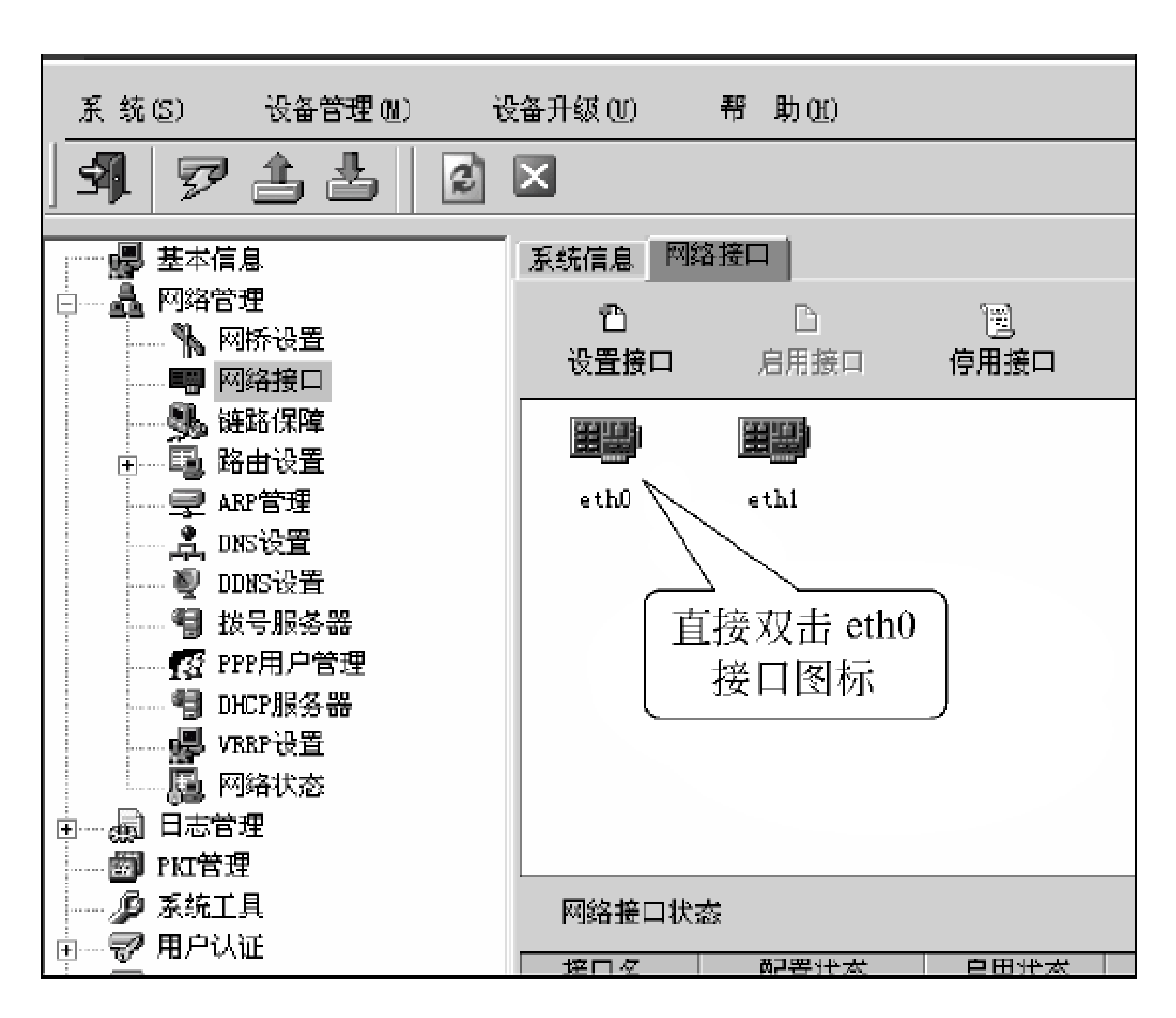


图 2-34　配置 VPN 网关 eth0 口地址(1)

按照对话框提示的要求,设置 eth0 接口地址,如图 2-35 所示。



图 2-35　配置 VPN 网关 eth0 口地址(2)

第三步：生成 VPN 网关数字证书。

（1）在图 2-34 所示 VPN 管理软件主界面上，选择“PKI 管理”功能，进入“PKI 管理”界面，如图 2-36 所示。



图 2-36　选择“PKI 管理”界面

（2）打开“PKI 管理”界面，单击“生成设备证书”按钮，按照界面提示输入信息，如图 2-37 所示。



图 2-37　生成设备证书配置

（3）单击“确定”按钮后，系统会提示证书生成成功，并要求保存配置，否则系统重启后，证书信息将丢失，如图 2-38 所示。

在图 2-34 所示 VPN 管理软件主界面上，选择“设备管理”主菜单功能，执行“保存配置”操作，如图 2-39 所示。

新生成的数字证书需要执行一次“重载设备证书”的操作，否则 VPN 系统并没有将该数字证书生效。在图 2-34 VPN 管理软件主界面上，选择“虚拟专用网”菜单项，打开 IPSec VPN 功能项，双击“重载设备证书”，操作如图 2-40 所示。

在打开的对话框中，因没有建立隧道，所以该提示可以忽略，单击“确定”按钮后，提示重载操作成功，如图 2-41 所示。

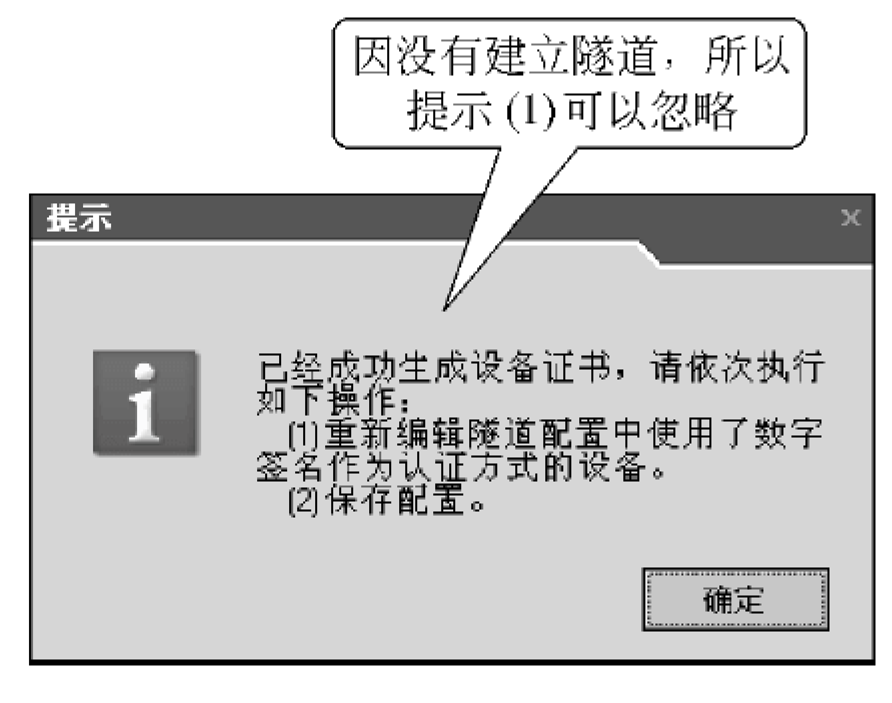


图 2-38　生成设备证书

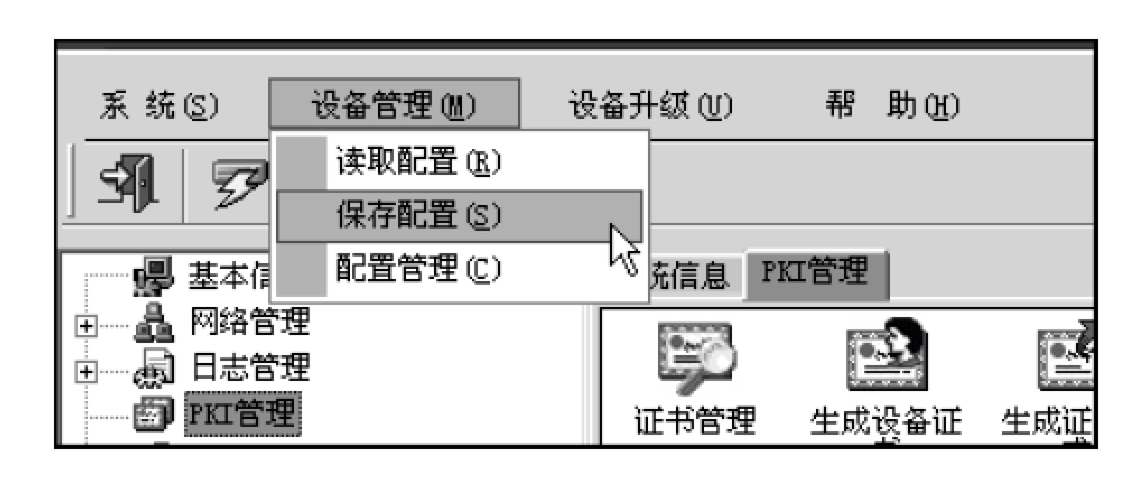
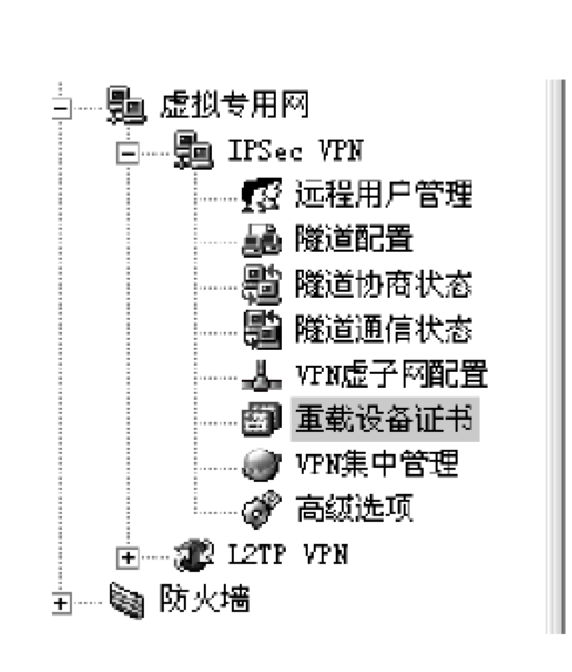


图 2-39　保存配置操作



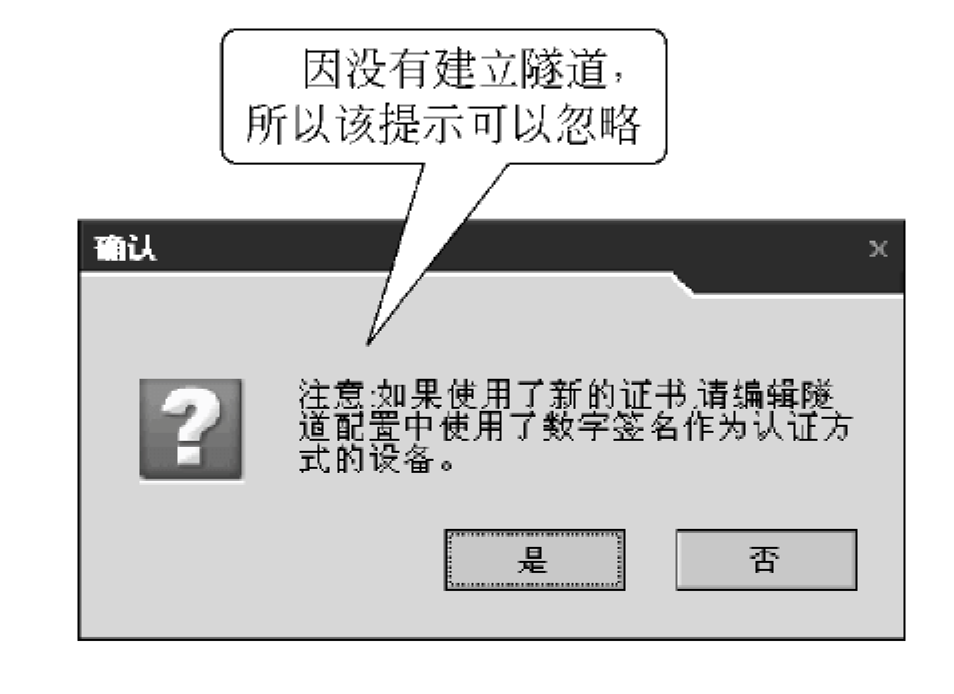


图 2-40　重载设备证书

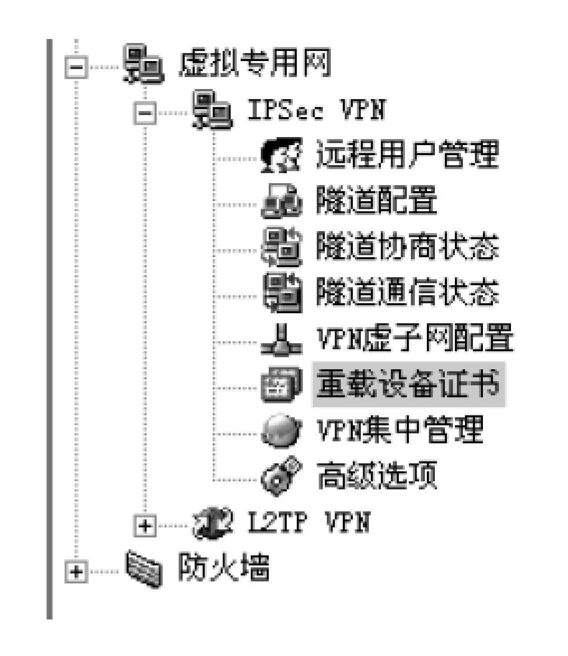




图 2-41　重载设备证书完成

(4) 新生成的设备证书可以在图 2-36 所示的 PKI 界面的“证书管理”中查看到。

在图 2-34 所示 VPN 管理软件主界面上，选择“PKI 管理”功能项，双击“证书管理”，即可查看证书信息，如图 2-42 所示。

注意：数字证书通常由 CA 中心来颁发，本实验中 RG-CMS 充当的是 CA 中心的角色，因此 VPN 网关的数字证书应该由 RG-CMS 来颁发。

为了简化操作，在锐捷 VPN 网关中，预置了 CA 的颁发数字证书的功能，预先定义了 CA 中心的默认根 CA(即锐捷根 CA)。可以通过图 2-36 所示 PKI 界面的“证书管理”→“证书颁发机构”标签，查看到该默认的锐捷根 CA，如图 2-43 所示。

因此本实验中，CA 中心的根 CA 选择了默认的锐捷根 CA。直接在 VPN 网关上生

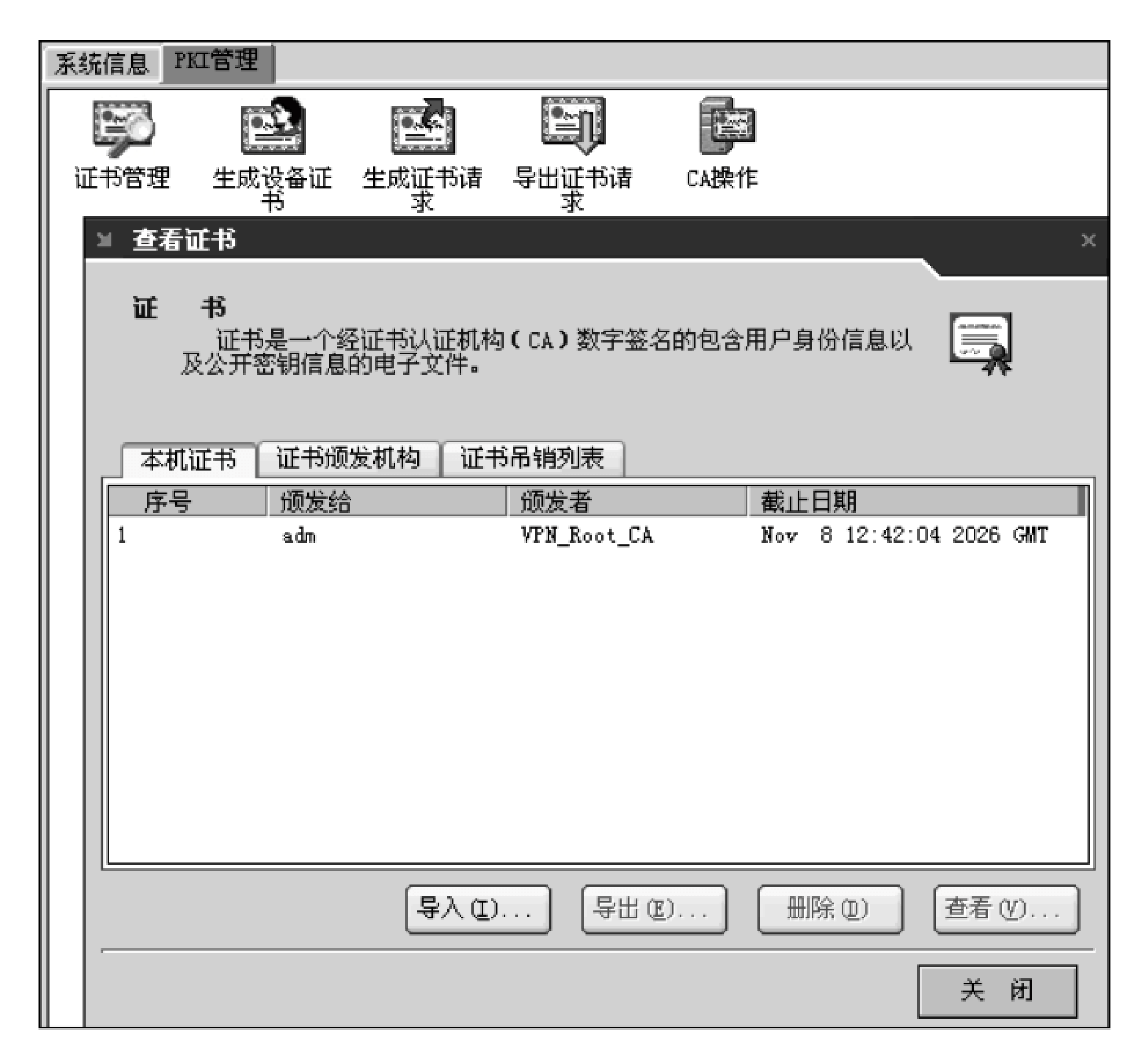


图 2-42　查看证书信息

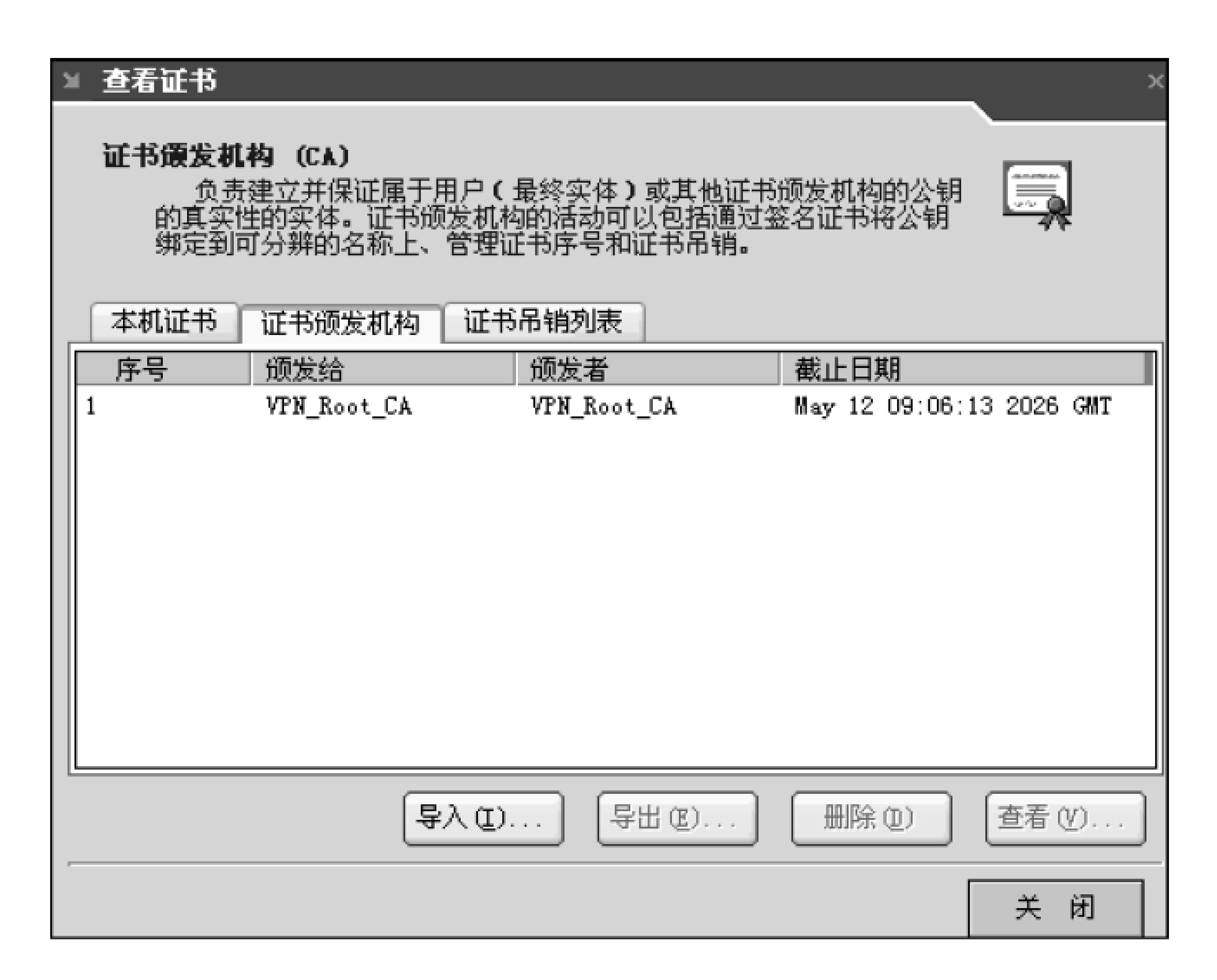


图 2-43　查看证书颁发机构信息

成 VPN 网关的数字证书。

第五步中使用 RG-CMS 为移动用户(即 PC 用户)生成数字证书时,注意其 CA 根证书也要采用锐捷默认根 CA。在第一次运行 RG-CMS 时,系统会给出 CA 根证书的提示信息。一旦选择错误,需要卸载 RG-CMS 后再重新安装,并重新选择。

第四步:配置 IPSec VPN 隧道。

(1) 进入远程移动用户 VPN 隧道配置界面。

登录 VPN 网关的管理界面,在图 2-34 所示的 VPN 管理软件主界面上,选择“虚拟专

用网”菜单项,打开 IPSec VPN 功能项,双击“远程用户管理”项,打开“远程用户管理”界面,操作如图 2-44 所示。

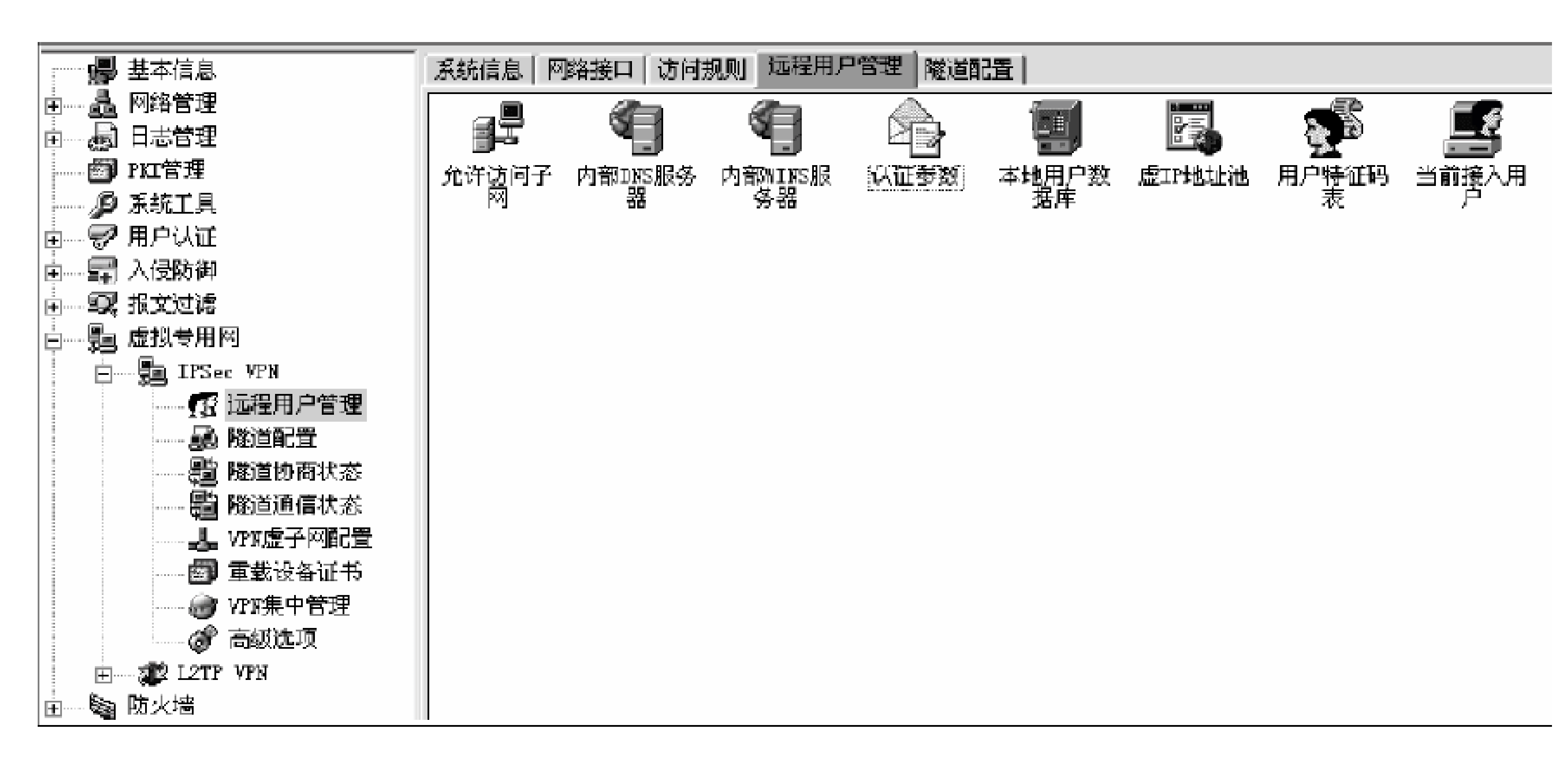


图 2-44 打开“远程用户管理”功能

(2) 配置“允许访问子网”。

在打开的“远程用户管理”界面上配置“允许访问子网”功能,配置“允许访问子网”,操作如图 2-45 所示。

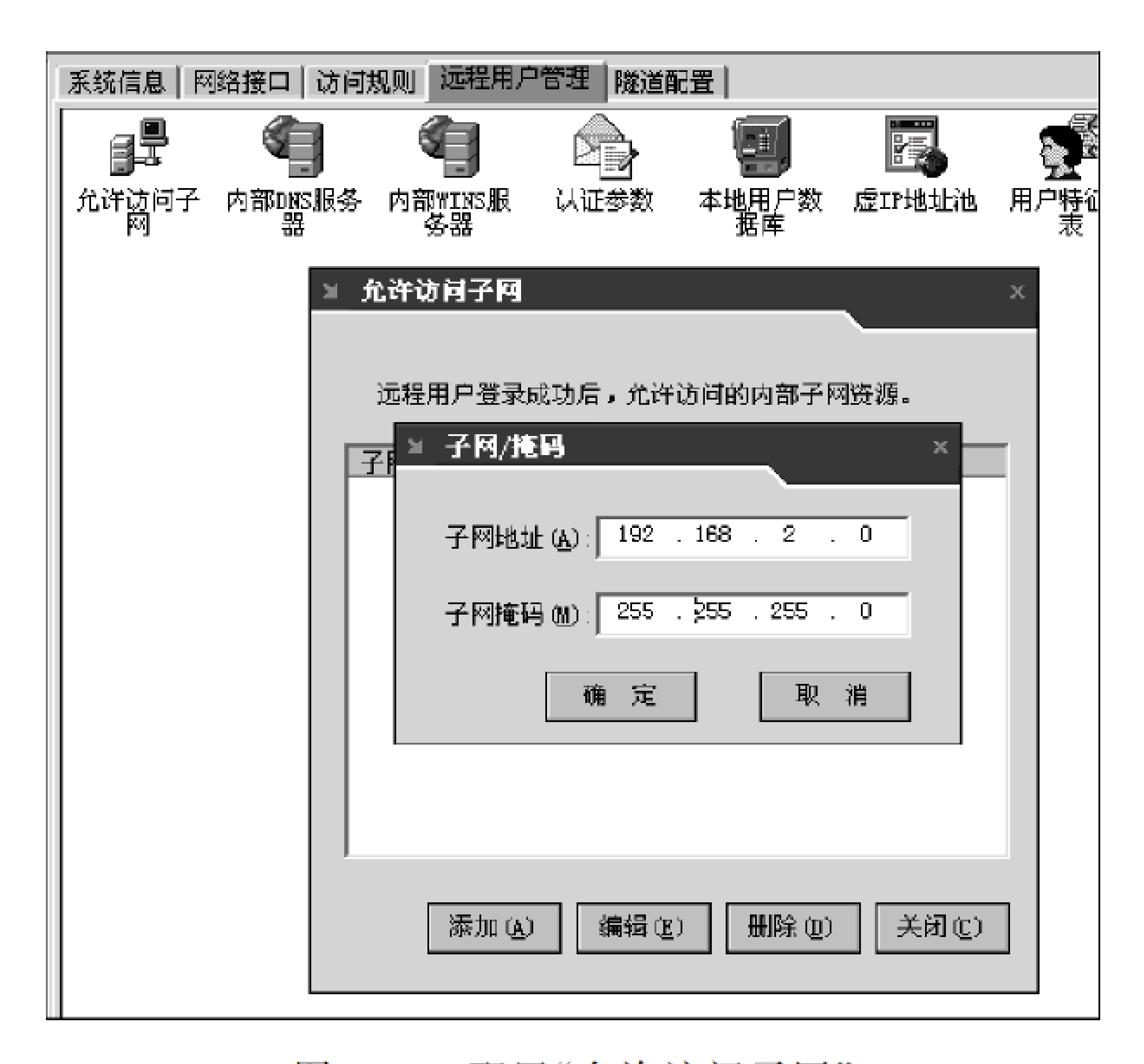


图 2-45 配置“允许访问子网”

在图 2-44 所示的“远程用户管理”界面上选择“认证参数配置”功能,配置认证参数,操作如图 2-46 所示。打开“认证参数配置”功能后,选择“证书认证配置”,提示认证证书根证书记录信息。

(3) 配置“虚 IP 地址池”。

在打开图 2-44 所示的“远程用户管理”界面上选择“虚 IP 地址池”功能项,配置虚 IP 地址池参数,操作如图 2-47 所示。



图 2-46　配置“认证参数配置”

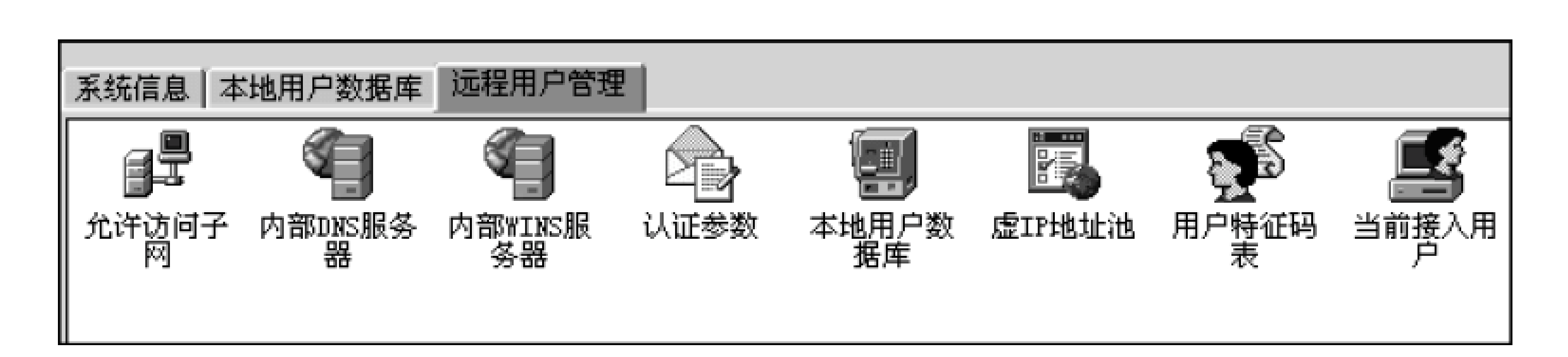


图 2-47　配置“虚 IP 地址池”

在打开的“虚 IP 地址池”界面上选择“虚 IP 地址池”，按“添加”按钮，配置子网地址的虚 IP 地址信息，如图 2-48 所示。



图 2-48　配置相关的虚 IP 地址信息

注意：分配 PC 的虚拟 IP 地址，既可以定义一个地址池，由 VPN 网关自动分配，也可以请管理员一个 IP 对应一个用户的分配，本实验选择地址池方式，由系统自动分配，并且选择定义“子网地址”的地址池。

虚 IP 是网络管理员分配给远程移动用户的 IP，表示只有拥有该 IP 的 PC 才能获得局域网内部的访问权限。因此，管理员设置的虚 IP 一定不要与远程 PC 的 IP 冲突，以及和局域网内部的 IP 互相冲突。否则远程 PC 在和 VPN 网关建立隧道后，因地址冲突的问题，也无法访问局域网内部的服务器。本实验中虚 IP 地址池选择定义一个完全没有使用的网段，如图 2-49 所示。

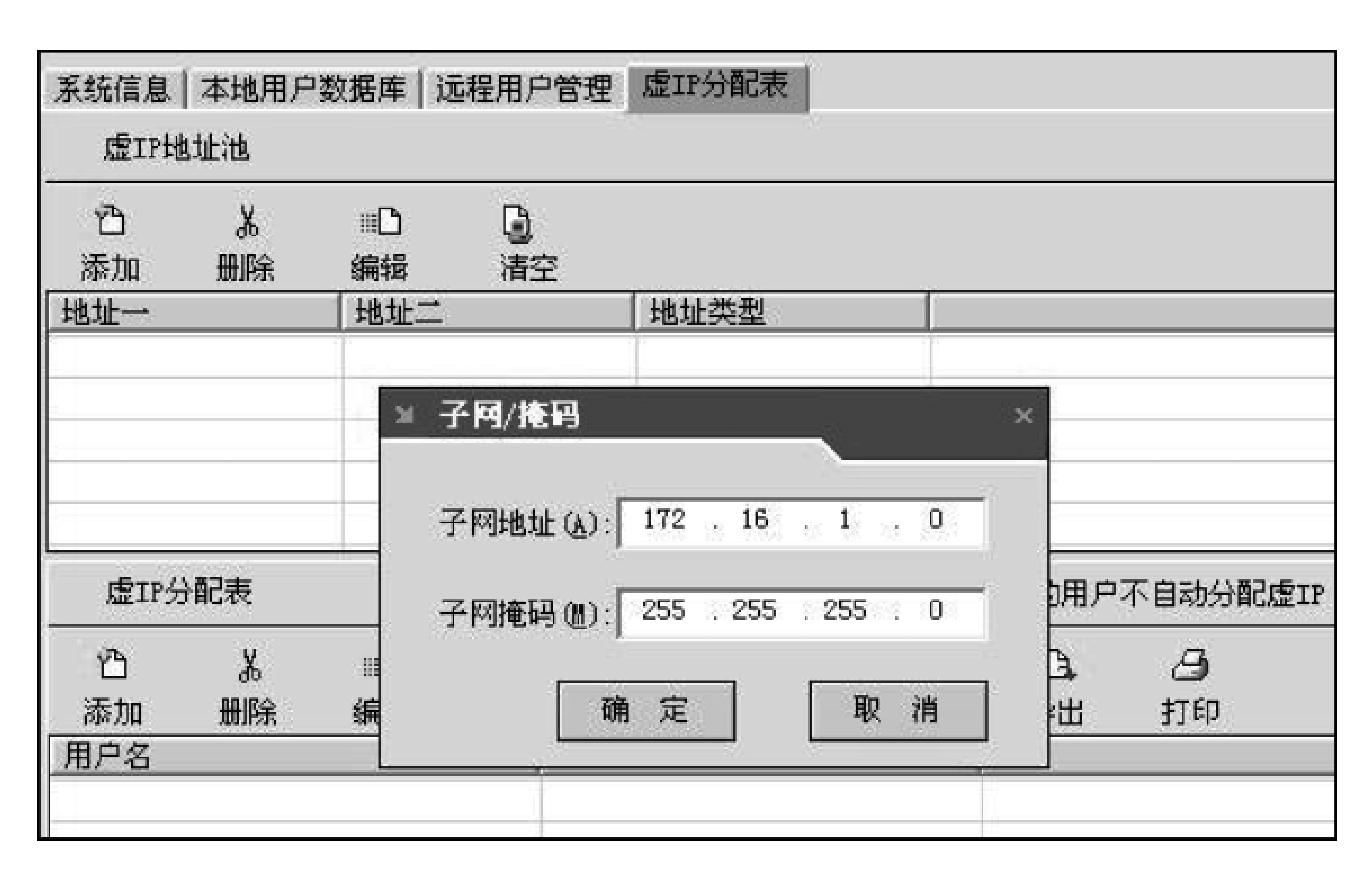


图 2-49　配置相关的虚 IP 地址信息

按“确定”后，如图 2-50 所示是配置成功的虚 IP 地址信息。

系统信息 | 本地用户数据库 | 远程用户管理 | 虚IP分配表

虚IP地址池

添加　删除　编辑　清空

地址一	地址二	地址类型
172.16.1.0	255.255.255.0	子网地址

图 2-50　配置成功的虚 IP 地址信息

(4) 配置“用户特征码”。

在打开图 2-47 所示“远程用户管理”界面上选择“用户特征码”功能，配置用户特征码参数，操作如图 2-51 所示。



图 2-51　配置用户特征码信息

打开“用户特征码”配置界面，选择配置“允许接入”功能，配置用户特征码接入参数，

操作如图 2-52 所示。

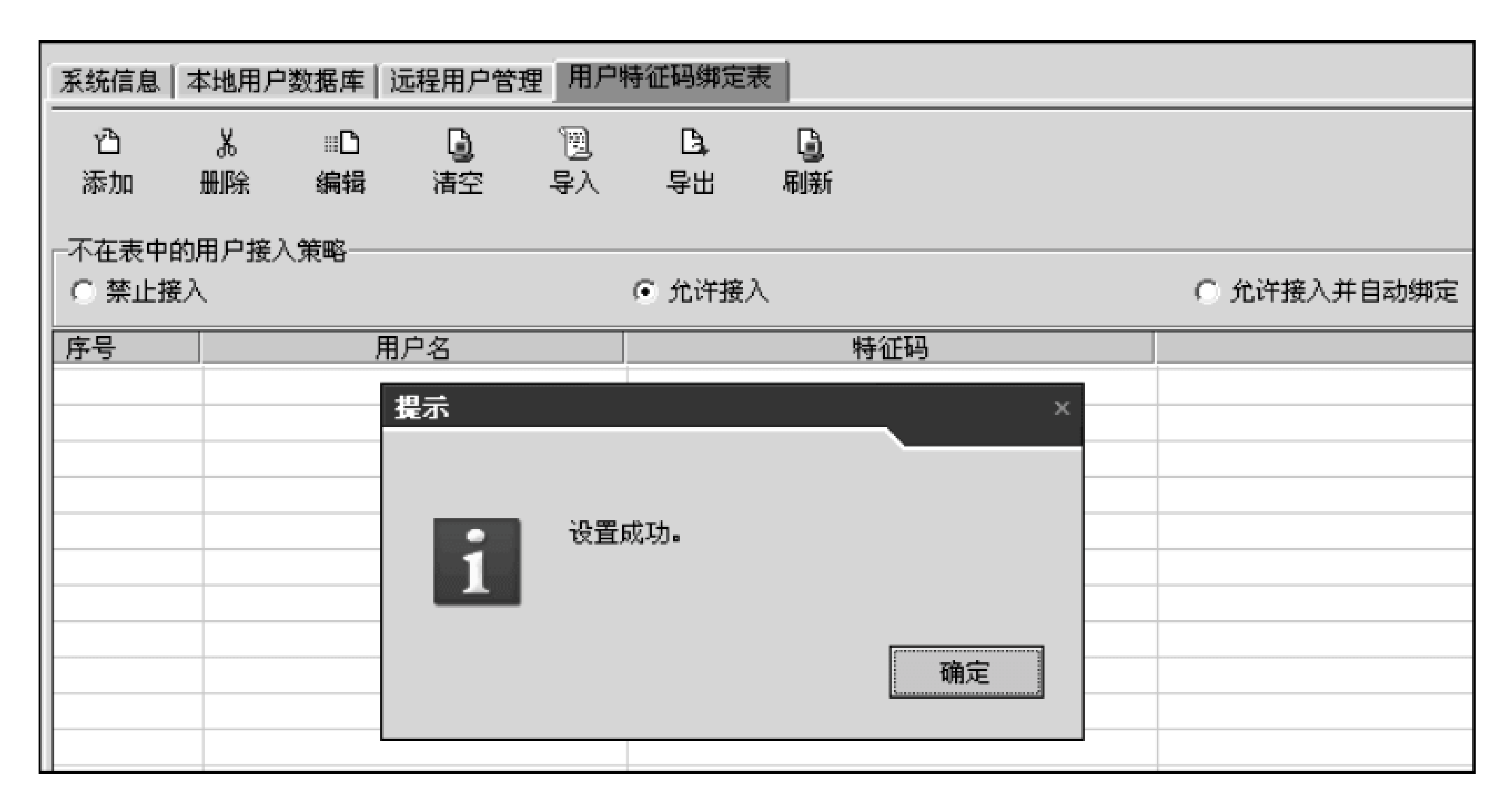


图 2-52　配置允许用户接入特征码

配置说明："用户特征码表"是为将远程 PC 的硬件和分配给用户身份信息绑定需求而设计的。如果选择图 2-52 上"允许接入并自动绑定"功能，则 VPN 网关会将远程用户的 PC 硬件特征码与该用户的身份认证信息相互绑定，绑定后该用户将无法用自己的身份信息再在其他 PC 设备上建立 VPN 隧道。

本实验中既可以选择"允许接入"，也可以选择"允许接入并自动绑定"。系统默认配置是"禁止接入"。图 2-52 上选择的是"允许接入"项，这表示该用户的身份信息不会和其使用的 PC 硬件绑定。

此次实验，"远程用户管理"界面的其他配置项，例如，"内部 DNS 服务器"、"内部 WINS 服务器"、"认证参数"，用户可以根据实际需要选择设置。但该实验因为不涉及这些应用，故不需要进行设置。

第五步：为远程接入用户颁发数字证书。

（1）在服务器上运行 RG-CMS 程序。

第一次运行 RG-CMS 时，系统会提示选择使用哪种 CA 根证书。因该实验采用的是系统默认的锐捷根 CA，因此按照如图 2-53 所示做选择。

（2）在打开的"RG-CMS 程序"中，进入 RG-CMS 后，打开"用户操作"菜单，先添加一个新用户，如图 2-54 所示。



图 2-53　运行 RG-CMS 程序



图 2-54　添加一个新用户

在如图 2-55 所示的“用户信息”界面上,根据提示,输入全部的信息。

用户信息
国家 cn
省/直辖市 bj
城市/地区 bj
组织 ruijie
部门 test
用户 pc1
电子邮件 pc1@ruijie.com.cn
用户类型 客户端用户
确定(O)　取消(C)
为移动用户颁发证书一定要选择“客户端用户”

图 2-55　输入新用户信息

(3) 添加完用户后,执行生成该用户数字证书的操作。

在图 2-54 所示的“RG-CMS 程序”主界面上,打开左侧“证书管理系统”菜单,选择加入的新用户,右击出现快捷菜单,选择“生成证书”命令,如图 2-56 所示。



图 2-56　为添加新用户生成证书

(4) 将数字证书写入 RG-Key 设备中。

① 将 RG-Key 设备先插入服务器的 USB 口。

② 在“证书管理系统”主界面上,选中该用户证书并右击,在弹出的快捷菜单中选择“导出证书和私钥”命令,如图 2-57 所示。

③ 选择“写入 RG-Key”选项。

在打开“导出证书和私钥”对话框中,选择导出证书类型和写入类型,如图 2-58 所示。

④ 在“导出证书类型”对话框中,根据如图 2-59 所示界面提示,输入 RG-Key 的 PIN 号(锐捷 RG-Key 出厂的默认 PIN 号是 ruijie)。

单击“确定”按钮后,系统开始写私钥文件,私钥写入RG-Key后,界面会提示是否要

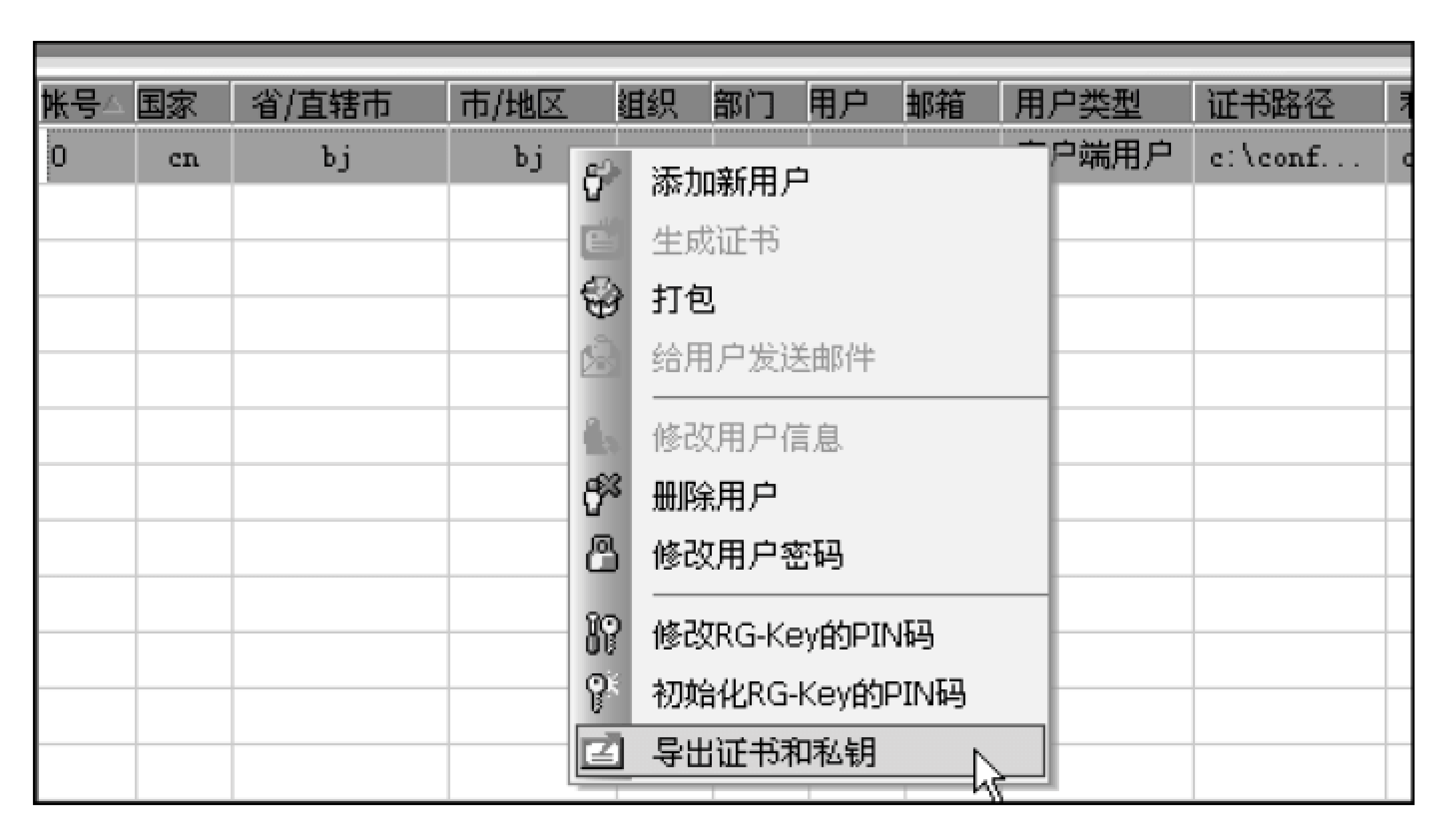


图 2-57　导出证书和私钥

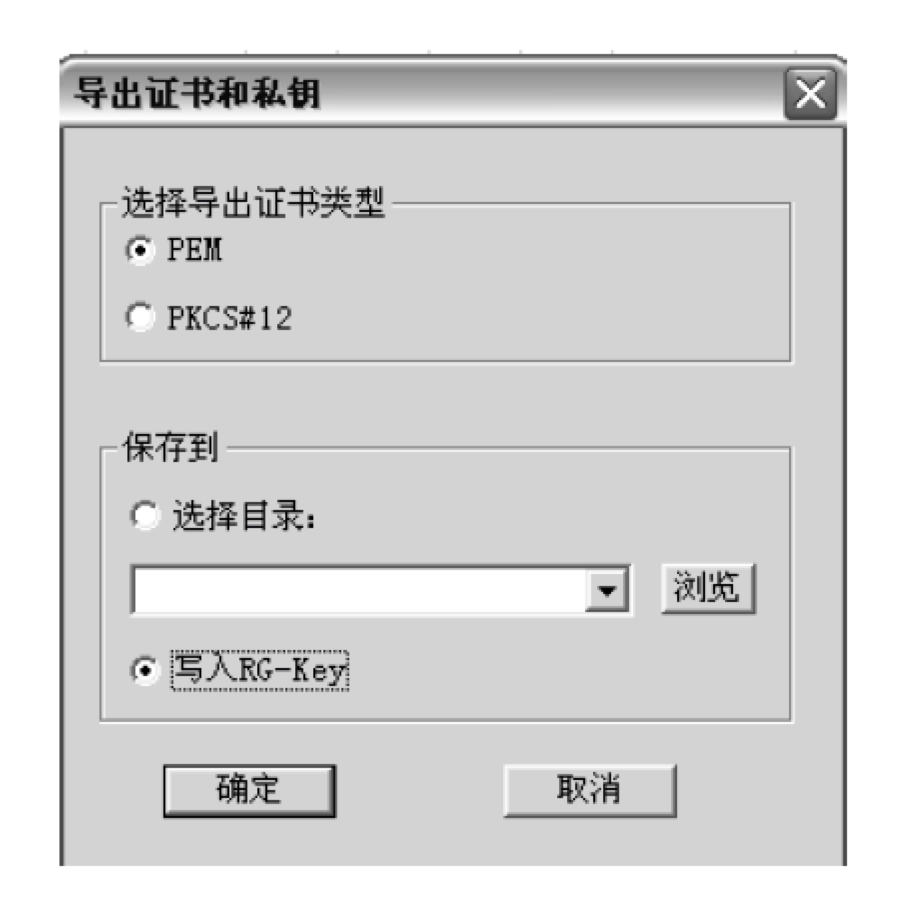


图 2-58　选择导出证书类型和写入类型



图 2-59　输入 RG-Key 的 PIN 号

写“证书”文件，请选择“是”，如图 2-60 所示。

至此，移动用户的数字证书信息已全部写入了 RG-Key 设备，如图 2-61 所示。



图 2-60　写入 RG-Key 私钥文件



图 2-61　写入 RG-Key 私钥文件成功

第六步：配置远程接入客户端。

(1) 第一次运行 RG-SRA 程序后，如图 2-62 所示。

(2) 建立一个与 VPN 网关的隧道连接。

在运行 RG-SRA 程序主界面上，单击“新建连接”按钮，建立一个与 VPN 网关的隧道连接，如图 2-63 所示。填写新建 VPN 网关的隧道连接的基本信息：连接标示、服务器地址、认证方式等，如图 2-64 所示。

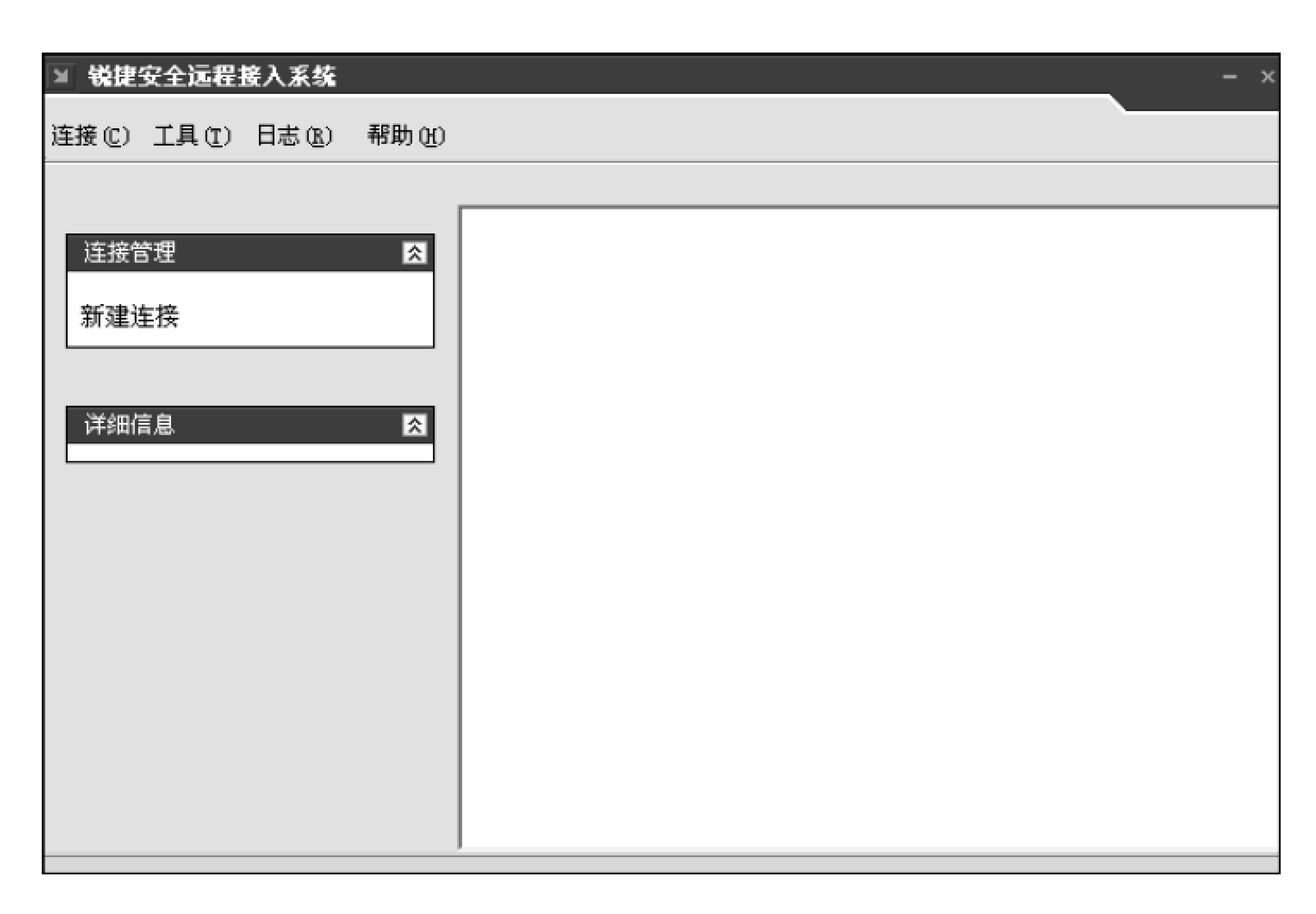


图 2-62　运行 RG-SRA 程序



图 2-63　新建隧道连接

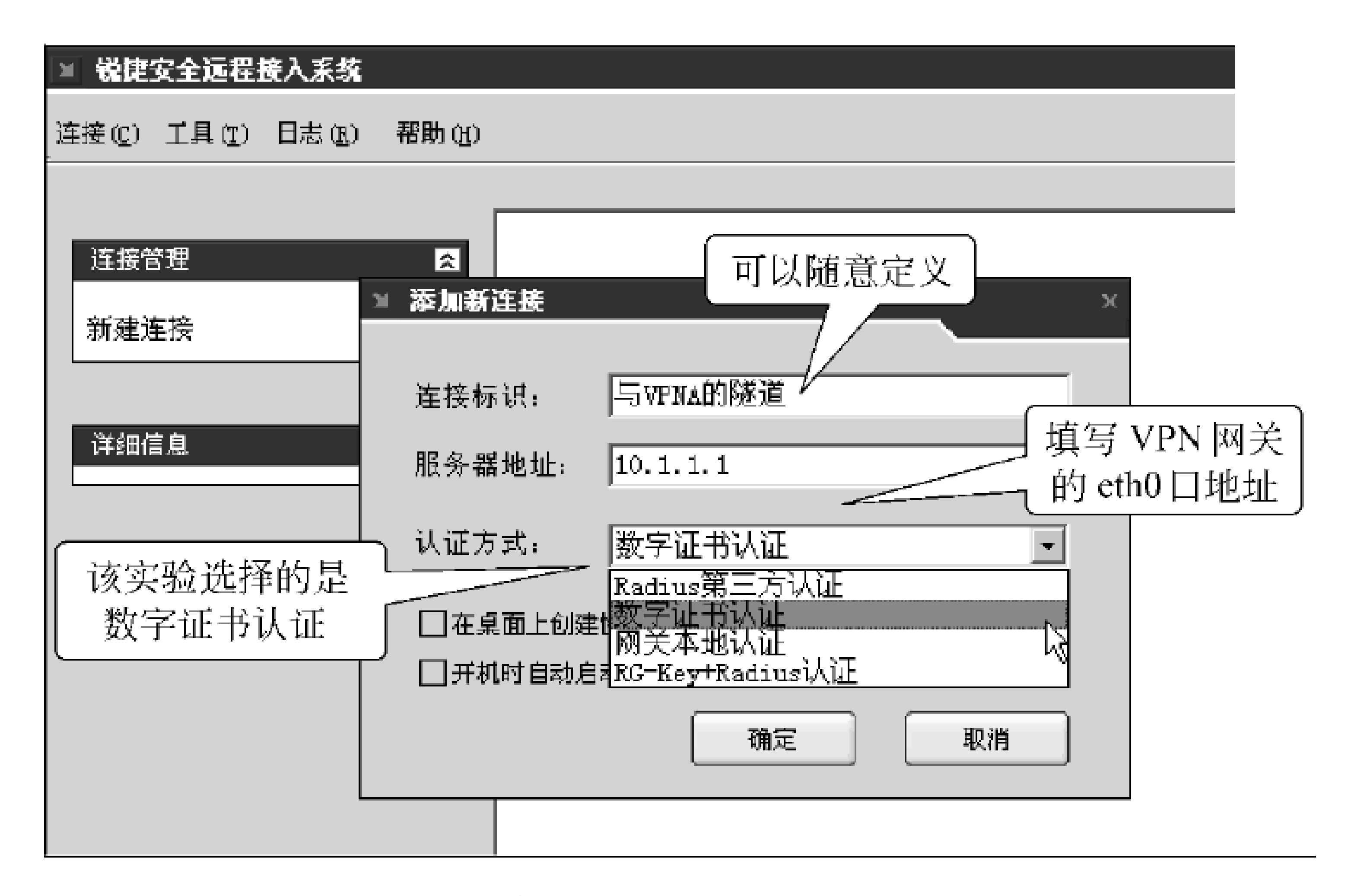


图 2-64　填写新建 VPN 网关的隧道连接的基本信息

如图 2-65 所示是配置成功"新建 VPN 网关的隧道连接"基本信息。

单击"确定"按钮后，显示建立完成的一个与 VPN 网关的隧道连接标号，如图 2-66 所示。

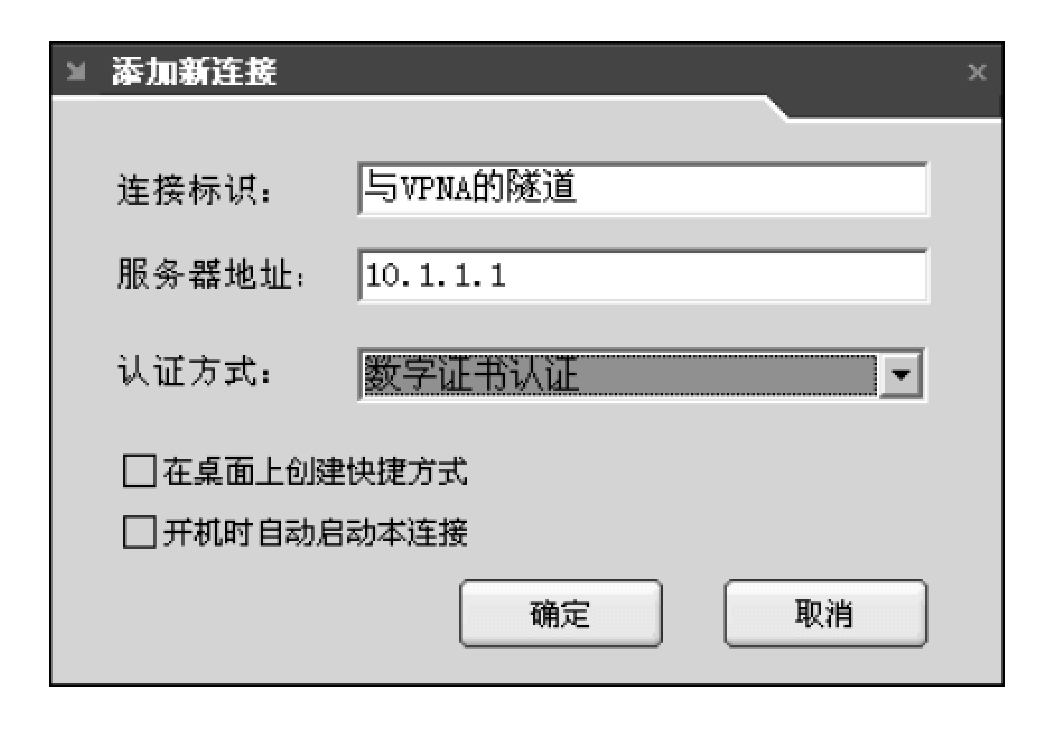


图 2-65 配置成功隧道连接



图 2-66 建立完成 VPN 网关的隧道连接

(3) 将 RG-Key 插入 PC 的 USB 口。

(4) 运行图 2-66 上所示的该隧道连接，建立 VPN 隧道。

在运行 RG-SRA 程序主界面上单击"连接管理"按钮，管理新建立 VPN 网关的隧道连接，右击打开快捷菜单，选择"启动连接"命令，启动新建的隧道连接，如图 2-67 所示。

通过"启动连接"命令，启动新建的隧道连接后，打开如图 2-68 所示 VPN 远程连接对话框，单击"获得证书"按钮。

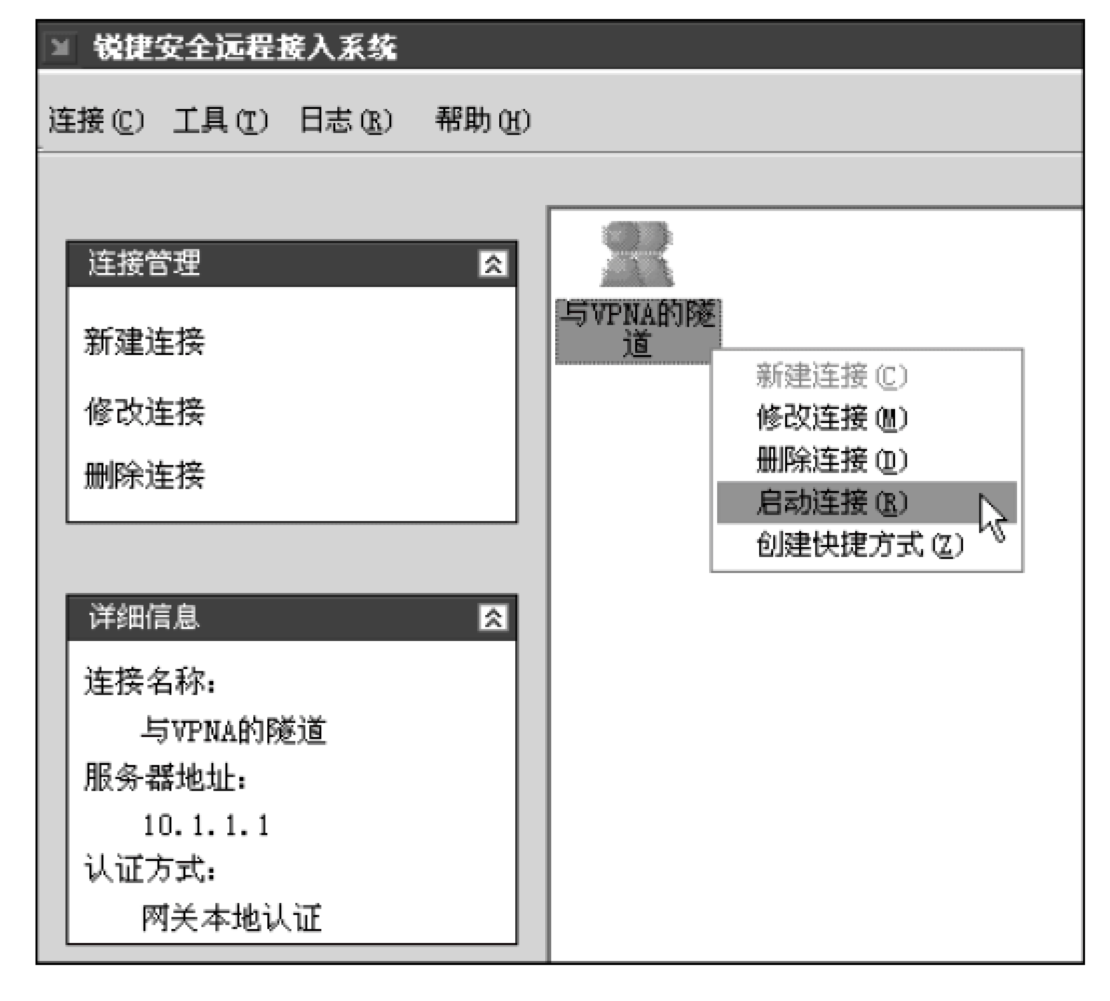


图 2-67 启动新建 VPN 网关隧道连接



图 2-68 获得 VPN 远程连接证书

在打开"获得证书"对话框中，在证书导入方式中，选择"从 RG-Key 中读取"选项，如图 2-69 所示。

确定后，在"输入 pin 码"框中输入 RG-Key 的 pin 号，如图 2-70 所示。

单击"连接"按钮后，系统自动进行身份认证，并且开始 IKE 的协商，如图 2-71 所示。

完成身份认证和隧道建立的过程后，RG-SRA程序会自动缩小图标显示在屏幕的右



图 2-69　选择获得证书方式



图 2-70　输入 RG-Key 的 pin 号



图 2-71　系统自动进行身份认证

下角，如图 2-72 所示。

选择 SRA 程序运行成功缩小图标，右击打开快捷菜单，在菜单中选择“详细配置”，可以查看到隧道信息，如图 2-73 所示。



图 2-72　连接成功缩小图标



图 2-73　查看到隧道信息

如图 2-74 所示信息为查看到隧道连接信息，显示“可访问”表示隧道已建立成功，如果是“不可访问”则表示隧道没有建立成功。“资源信息”中显示的“虚拟 IP 地址”信息，表

示该 IP 为 VPN 网关从虚地址池中自动分配给该 PC 的虚 IP。

第七步：验证测试。

在 VPN 网关的管理界面也可看到已经建立成功的隧道信息。

如图 2-75 所示隧道启动后，在 VPN 管理主界面上的“隧道协商状态”栏目下，看到“隧道的协商状态”，打开后“隧道状态”显示“第二阶段协商成功”。

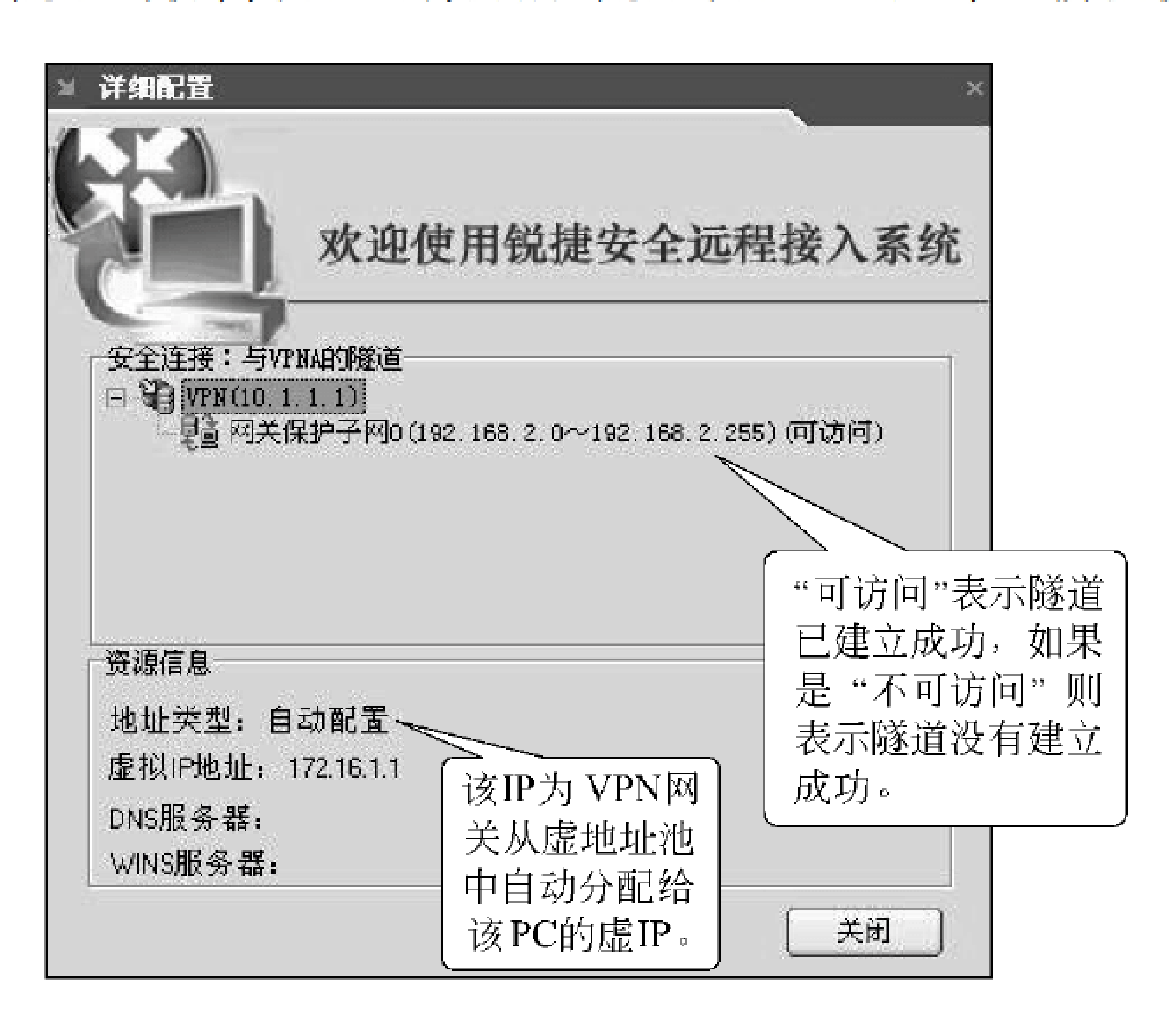


图 2-74　显示隧道配置信息内容

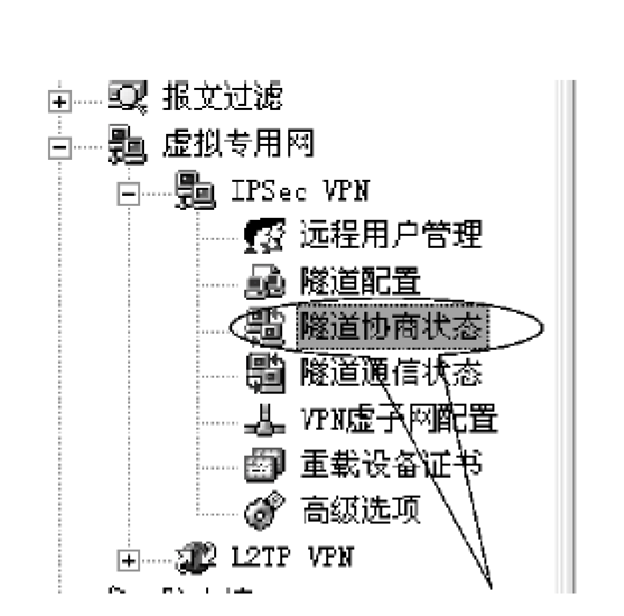


图 2-75　查看隧道协商信息

隧道启动后可以在“隧道协商状态”栏目下看到隧道的协商状态，“隧道状态”显示“第二阶段协商成功”。VPN 隧道的通信情况可以在“隧道协商状态”栏中查看到，如图 2-76 所示。

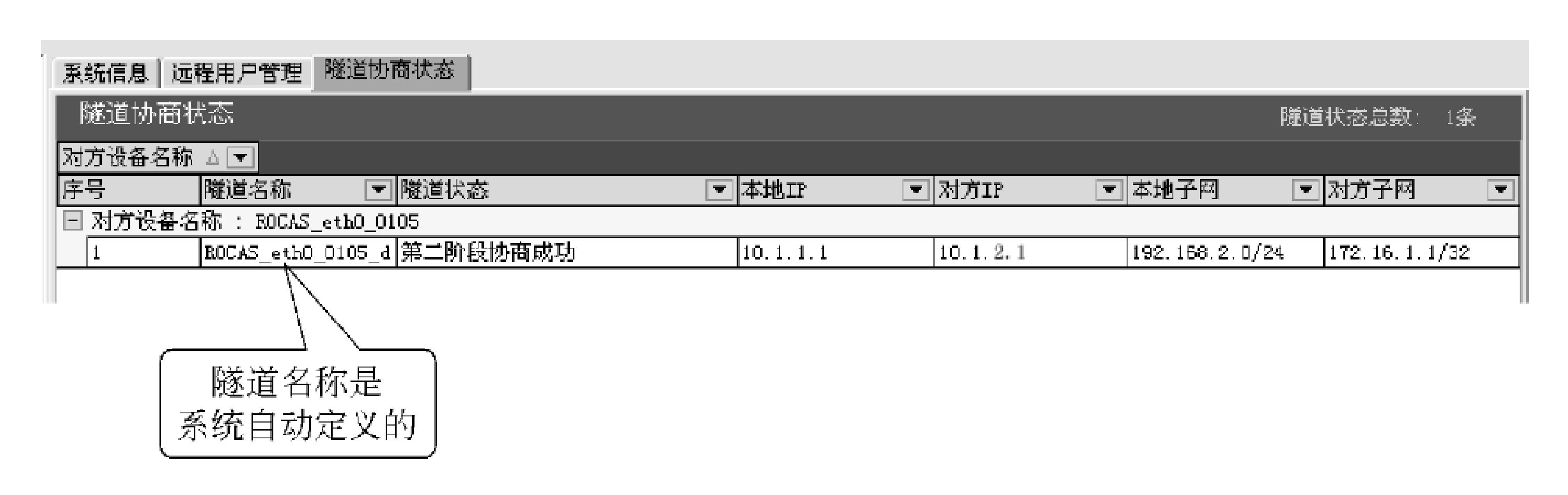


图 2-76　隧道协商状态

第八步：进行隧道通信。

在远程用户 PC 机上可以成功去访问服务器提供的服务，或者在 PC 上 ping 服务器的 IP 地址可以 ping 通(没有 VPN 隧道前 ping 会失败)。VPN 隧道的通信情况可以在 VPN 管理主界面上“隧道通信状态”中查看到，如图 2-77 所示。

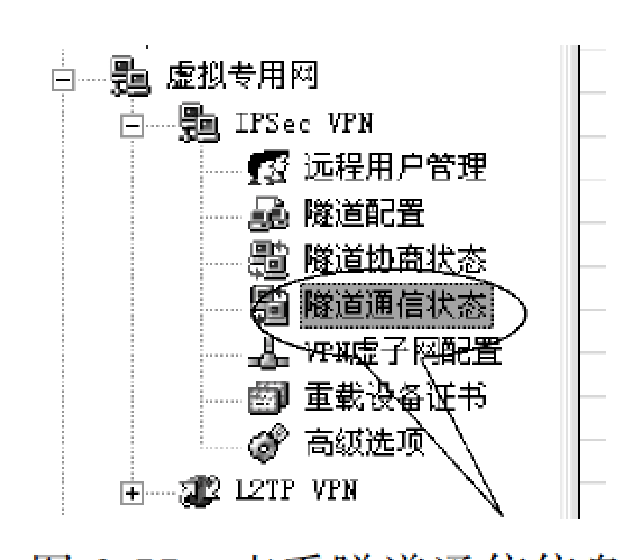


图 2-77　查看隧道通信信息

隧道启动后，在打开的“隧道通信状态”栏目下看到隧道的通信状态，“隧道状态”显示“第二阶段协商成功”。

VPN 隧道通信情况可以在“隧道通信状态”中查看到，如图 2-78 所示。

系统信息 | 网络接口 | 隧道配置 | 隧道通信状态 | 隧道协商状态 |

隧道通信状态

序号	类型	本地子网	对方子网	发送成功包数	发送失败包数	发送成功字节数
1	IKE	192.168.2.0/24	172.16.1.1/32	14	0	840

隧道通信统计

校验失败包数	发生重播包数	非法加密包数
0	0	0

图 2-78　隧道通信状态

【注意事项】

- 实验环境地址可以随意定义，但请不要使用 1.1.1.0 这个网段的 IP，因为某些功能实现的需要，VPN 系统内部已占用该网段的部分 IP。
- 该实验中，VPN 网关的防火墙规则为全部开放。但在实际的网络环境中，如果 VPN 网关直接连接 Internet 网络，则一定需要启用防火墙规则。
- RG-SRA 是 VPN 客户端软件程序，如果 PC 上已预装其他厂家的 VPN 客户端程序，请先卸载其他厂家的 VPN 客户端程序，否则可能 RG-SRA 无法正常工作。
- RG-SRA 作为安全产品，安装后会对系统的网卡、端口、协议等方面有改动，因此会和部分防火墙或者防病毒程序不兼容。推荐用户使用没有安装任何第三方防火墙、防病毒程序的机器来做实验。

2.3　实现远程访问 IPSec VPN 的授权控制

【实验名称】

实现远程访问 IPSec VPN 的授权控制。

【实验目的】

学习配置远程访问 IPSec VPN 隧道，熟悉远程接入方式下的 VPN 隧道建立过程。

【背景描述】

某员工在外地出差，需要访问公司内网中的服务器资源，而这些服务器资源因安全性考虑并不直接在公网 Internet 上开放，因此该员工必须通过先和公司建立 VPN 隧道，获得访问内部资源的权力后才能访问。

【需求分析】

需求：解决出差在外员工和公司内网之间，通过 Internet 进行数据传输的安全问题。

分析：IPSec VPN 技术通过隧道技术、加解密技术、密钥管理技术、认证技术等有效地保证了数据在 Internet 中传输的安全性，是目前最安全、使用最广泛的 VPN 技术。可以通过建立远程访问的 IPSec VPN 加密隧道，实现出差员工和公司之间安全的数据传输。

【实验拓扑】

如图 2-79 所示网络拓扑，是某公司员工正在外地出差，需要访问公司内网中的服务器资源。由于通过 Internet 数据传输的安全问题，公司内网中服务器资源因安全性考虑不直接在公网上开放。外地远程访问公司的内网中各种网络资源，通过 Internet 传输保密数据，公司希望通过建立 IPSec VPN 隧道加密传输。因此出差在外的员工必须先和公司建立 VPN 隧道，获得访问内部资源的权力，通过 IPSec VPN 隧道实现和公司内网之间安全的数据传输。

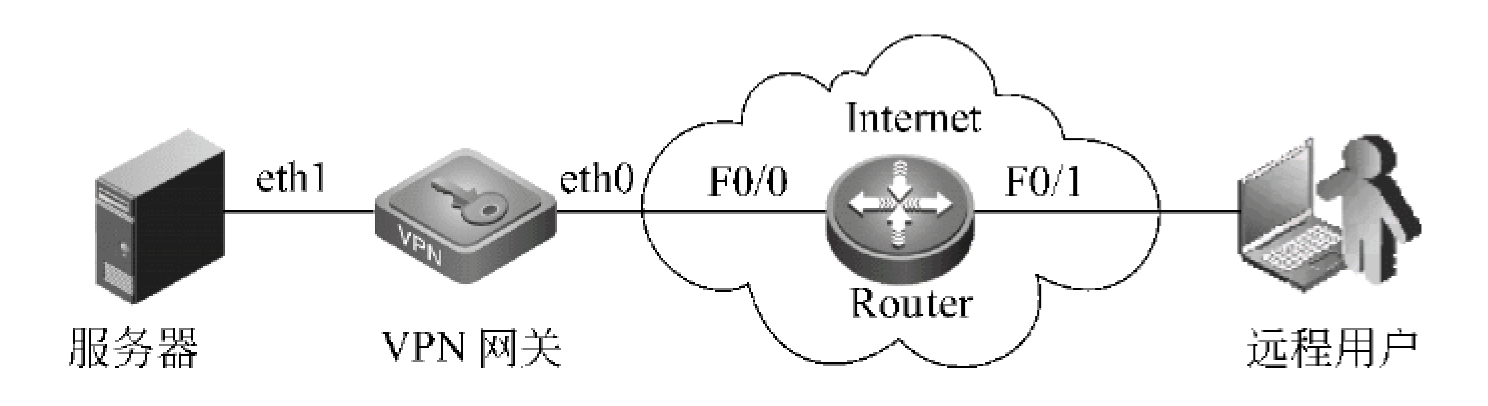


图 2-79　远程访问 IPSec VPN 的授权控制网络拓扑

【实验设备】

RG-WALL VPN 网关：1 台；RG-SRA 安全远程接入系统软件：1 套；路由器：1 台；PC：2 台(1 台作为公司内部服务器，1 台作为远程接入用户并安装 SRA 软件)。

【预备知识】

第二层隧道协议 L2TP

VPN 安全的具体实现是采用隧道技术，将企业网中保密的数据封装在 VPN 隧道中进行传输。VPN 隧道协议可分为第二层隧道协议 PPTP、L2F、L2TP 和第三层隧道协议 GRE、IPSec。它们本质区别在于用户的数据包是被封装在哪种类型的数据包中，再在隧道中传输。

1. PPTP 点对点隧道协议

PPTP 提供 PPTP 客户机和 PPTP 服务器之间的加密通信。PPTP 客户机是指运行了该协议的 PC，如启动该协议的 Windows XP。PPTP 服务器是指运行该协议的服务器，如启动该协议的 Windows NT 服务器。PPTP 可看做是 PPP 协议的一种扩展，它提供了一种在 Internet 上建立多协议的安全 VPN 通信方式。远端用户能够通过任何支持 PPTP 隧道协议的网络服务提供商(ISP)设备，访问公司的内部专用网络。PPTP 客户机

可采用拨号方式接入公共 Internet 网络。拨号客户首先按常规方式拨号到 ISP 的接入服务器 NAS,建立 PPP 连接。在此基础上,客户再进行二次拨号,建立到 PPTP 服务器的连接,该连接称为 PPTP 隧道。该 PPTP 隧道实质上是基于 IP 协议上的另一个 PPP 连接,可以封装多种协议数据,包括 TCP/IP、IPX 和 NetBEUI。PPTP 隧道采用了基于 RSA 公司 RC4 的数据加密方法,保证了虚拟连接通道的安全性。对于直接连到 Internet 上的客户则不需要第一重 PPP 的拨号连接,可以直接与 PPTP 服务器建立虚拟通道。

2. L2F 第二层转发协议

L2F 是由 Cisco 公司提出的可以在多种传输媒介,如 ATM、帧中继、IP 网上建立多协议的全 VPN 通信方式。

远端用户能够通过任何类型的用户,采用拨号方式接入公共 IP 网络。建立的过程是:首先按常规方式拨号到 ISP 的接入服务器 NAS,建立 PPP 连接;NAS 根据用户名等信息,发起第二重连接,通向 HGW 服务器。在这整个的通信过程,隧道的配置、建立对用户是完全透明的。

3. L2TP 第二层隧道协议

L2TP 结合了 L2F 和 PPTP 协议的优点,可以让用户从客户端或访问服务器端发起 VPN 连接。L2TP 是把链路层 PPP 帧封装在公共网络(如 IP、ATM、帧中继)中进行隧道传输的封装协议。

目前用户在通过拨号访问 Internet 时,多使用动态方式得到合法的 IP 地址,L2TP 的好处在于支持多种协议,用户可以保留原有的 IPX、Appletalk 协议提供地址或 IP 地址。L2TP 还解决了多个 PPP 链路的捆绑问题,PPP 链路捆绑要求其成员均指向同一个 NAS,L2TP 可以使物理上连接到不同 NAS 的 PPP 链路,在逻辑上的终结点为同一个物理设备。L2TP 扩展了 PPP 连接,在传统方式中用户通过模拟电话线或 ISDN/ADSL 与网络访问服务器(NAS)建立一个第二层的连接,并在其上运行 PPP。其第二层连接的终结点和 PPP 会话的终结点在同一个设备上(如 NAS)。L2TP 作为 PPP 的扩展提供更强的功能,第二层连接的终结点和 PPP 会话的终结点可以是不同的设备。

L2TP 二层隧道协议主要由 LAC(L2TP Access Concentrator)和 LNS(L2TP Network Server)构成,LAC 支持客户端的 L2TP,用于发起呼叫、接收呼叫和建立隧道;LNS 是所有隧道的终点。在传统的 PPP 连接中,用户拨号连接的终点是 LAC,L2TP 使得 PPP 协议的终点延伸到 LNS。

L2TP 二层隧道协议的建立过程是:

(1) 用户通过公共电话网或 ADSL 拨号至本地的接入服务器 LAC,LAC 接收呼叫并进行基本的辨别,这一过程可以采用几种标准,如域名、呼叫线路识别(CLID)或拨号 ID 业务(DNIS)等。

(2) 当用户被确认为合法企业用户时,就建立一个通向 LNS 的拨号 VPN 隧道。

(3) 通过企业内部的安全服务器如 TACACS+、RADIUS 鉴定拨号用户身份。

(4) NS 与远程用户交换 PPP 信息,分配 IP 地址。

LNS 可采用企业私有地址(未注册的 IP 地址)或服务提供商提供的地址。内部源 IP 地址与目的地 IP 地址都通过网络服务提供商提供的 IP 网络,封装成 PPP 信息包传送,企业私有地址对提供者的网络来说是透明的。

(5) 端到端的数据传输。

与 PPTP 和 L2F 相比,L2TP 的优点在于提供了差错和流量控制。作为 PPP 协议的扩展协议,L2TP 支持 PPP 标准的安全认证和检查特性 CHAP 和 PAP 协议,对用户身份进行认证。L2TP 协议定义了数据包的加密传输,对于每个建立好的隧道,生成一个独一无二的随机钥匙,以便抵抗来自网络的欺骗性的攻击。

【实验原理】

IPSec 的主要作用是为 IP 数据通信提供安全服务。IPSec 不是一个单独协议,它是一套完整的体系框架,包括 AH、ESP 和 IKE 三个协议。IPSec 使用多种加密算法、散列算法、密钥交换方法等为 IP 数据流提供安全,提供数据的机密性、数据的完整性、数据源认证和反重放等安全服务保障。

使用 IPSec 可以构建两种不同接入方式的 VPN,即远程访问 VPN 和站点到站点 VPN,本实验中使用 IPSec 来构建远程访问 VPN 安全。

远程网络中用户 PC 与公司 VPN 网关,通过 IKE 自动协商建立起远程访问 IPSec VPN 加密隧道,使得远程用户 PC 能安全地访问到 VPN 网关所保护的内网中的服务器资源。

远程用户 PC 在和 VPN 网关建立 VPN 隧道前,需要先获得公司内网中 VPN 网关的身份验证许可,本实验采用的用户身份验证为口令验证方式,为远程用户提供接入认证。

远程用户 PC 在通过内网中 VPN 网关的身份验证后,VPN 网关会自动将建立 VPN 隧道(即 IKE 协商)所需要的配置下发给远程用户 PC,然后远程用户 PC 与 VPN 网关之间自动开始 IKE 协商,协商成功后 VPN 隧道即建立成功。整个过程系统自动完成,无需人为干预,是免配置的操作方式。

【实验步骤】

第一步:准备好 PC 和服务器。

在模拟远程用户 PC 上安装 SRA 远程接入软件,安装完成后,可能需要重新启动 PC 方可生效。

在模拟服务器 PC 上安装 VPN 管理软件。

具体的安装过程不在这里进行详述,可以查看产品的随机说品书和产品光盘。

第二步:搭建拓扑,配置 IP 地址。

按照如图 2-79 所示拓扑图,搭建实验拓扑,并根据如表 2-3 所示编址方案,配置实验中各设备的 IP 地址。

(1) 在模拟服务器的超级终端上,转到命令行状态,在命令行下配置 VPN 网关的 eth1 口地址,操作如图 2-80 所示(注意:VPN 网关出厂时 eth1 口默认地址为 192.168.1.1/24)。

表 2-3 设备 IP 地址

设 备	接 口	地 址
VPN 网关	eth1 接口地址	192.168.2.1
	eth0 接口地址	10.1.1.1
PC	PC 的 IP 地址	10.1.2.1
	PC 网关地址	10.1.2.2
服务器	服务器的 IP 地址	192.168.2.2
	服务器网关地址	192.168.2.1
Router	F0/0 地址	10.1.1.2
	F0/1 地址	10.1.2.2

说明：PC 及 Router 地址的配置方式不再详述。

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manu
al):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.2.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# _
```

图 2-80 配置 VPN 网关 eth1 口地址

(2) 打开模拟服务器，启动服务器上 VPN 管理软件，登录 VPN 网关，然后直接双击“eth0 接口”图标。

打开对话框，配置 eth0 口地址，操作如图 2-81 所示。

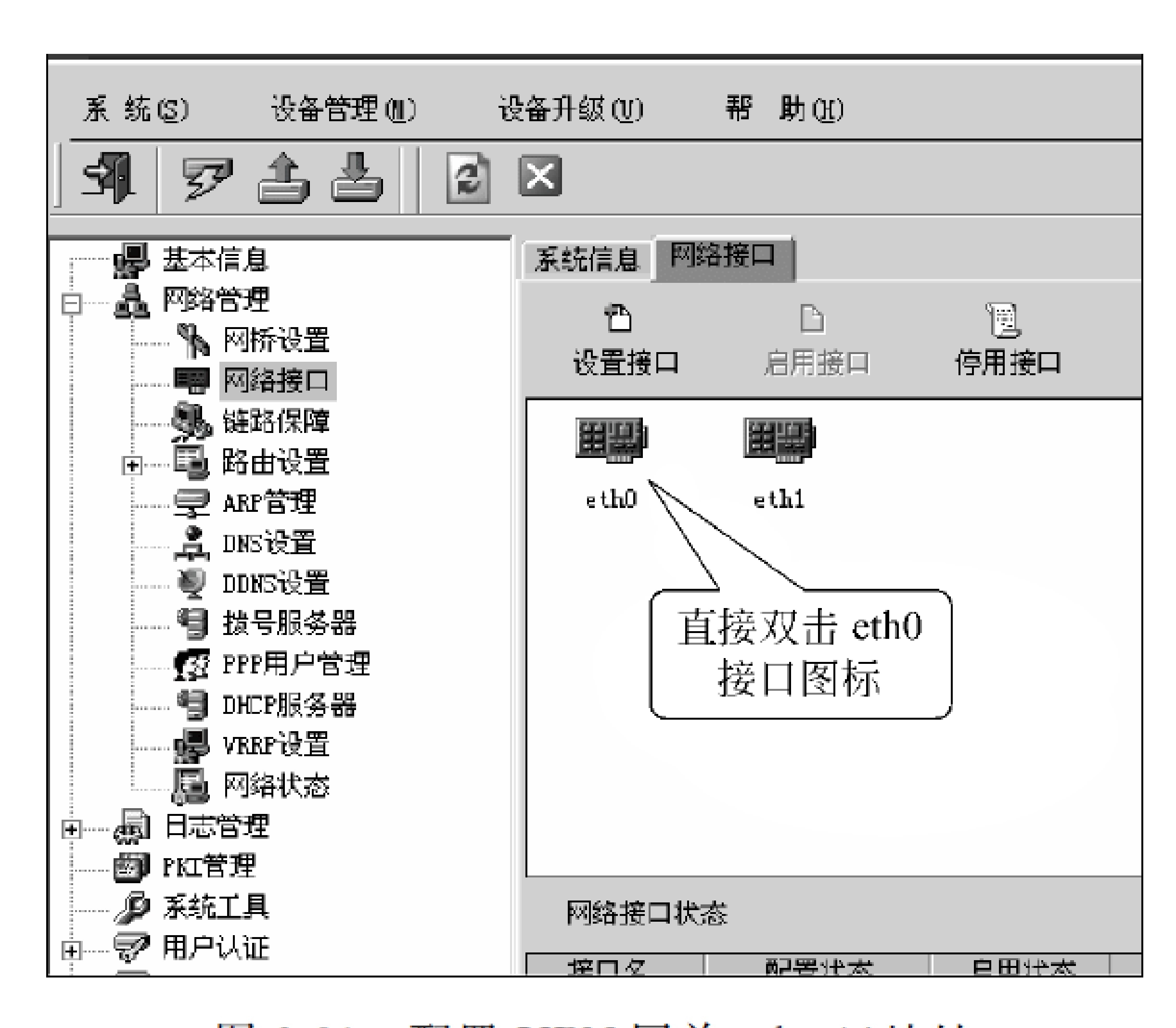


图 2-81 配置 VPN 网关 eth0 口地址

按照提示的要求设置 eth0 接口地址，如图 2-82 所示。



图 2-82　配置 VPN 网关 eth0 口地址

第三步：配置 IPSec VPN 隧道。

(1) 进入模拟远程移动用户 VPN 隧道配置的界面。

打开模拟远程用户 VPN 客户端软件，登录 VPN 网关的管理界面。在 VPN 管理软件主界面上，打开"虚拟专用网"菜单项，选择 IPSec VPN 功能项，双击"远程用户管理"选项，打开"远程用户管理"界面，操作如图 2-83 所示。

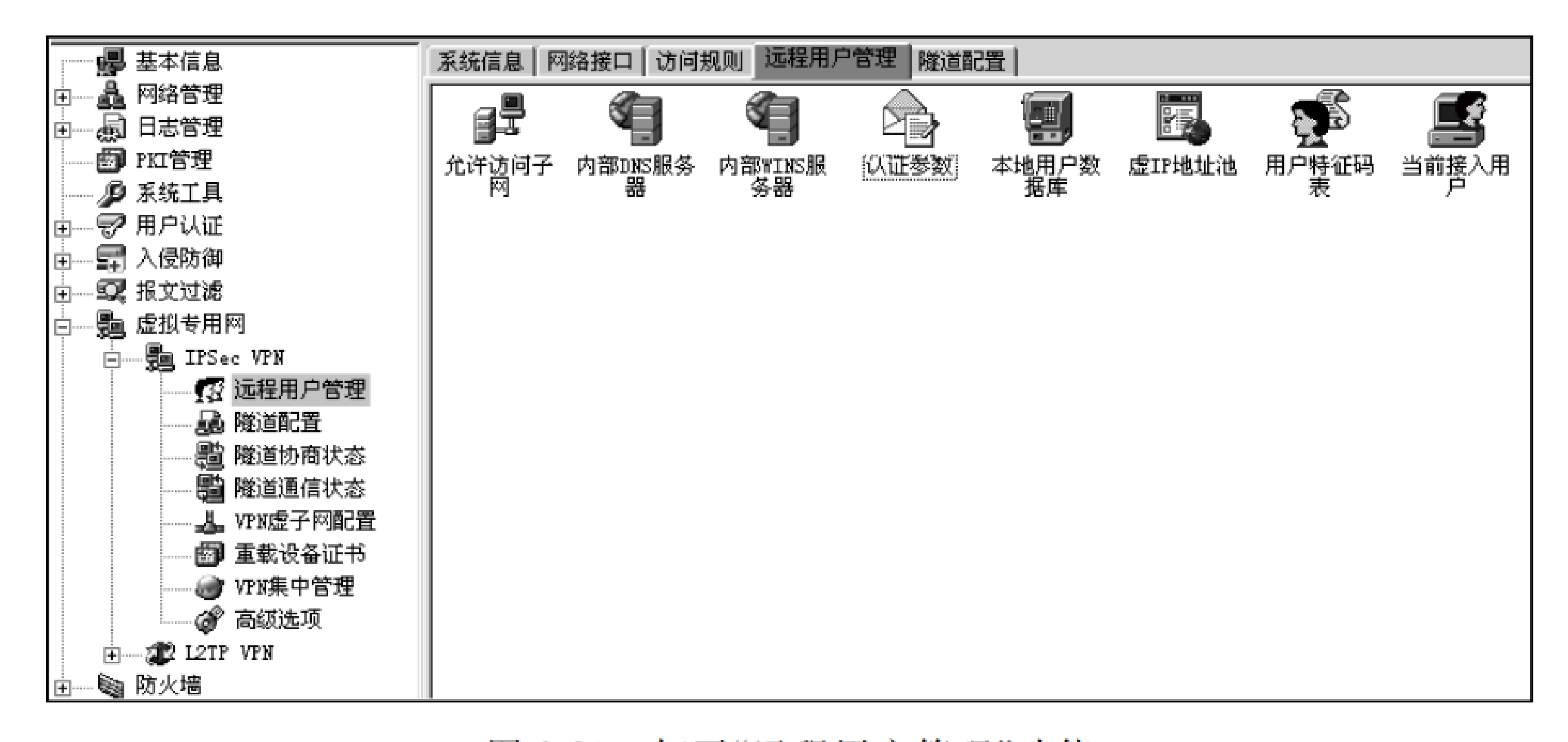


图 2-83　打开"远程用户管理"功能

(2) 配置"允许访问子网"。

在打开的"远程用户管理"界面上选择"允许访问子网"功能，配置允许访问子网，操作如图 2-84 所示。

(3) 配置"本地用户数据库"。

在打开的"远程用户管理"界面上选择"本地用户数据库"，配置本地用户数据库，如图 2-85 所示。

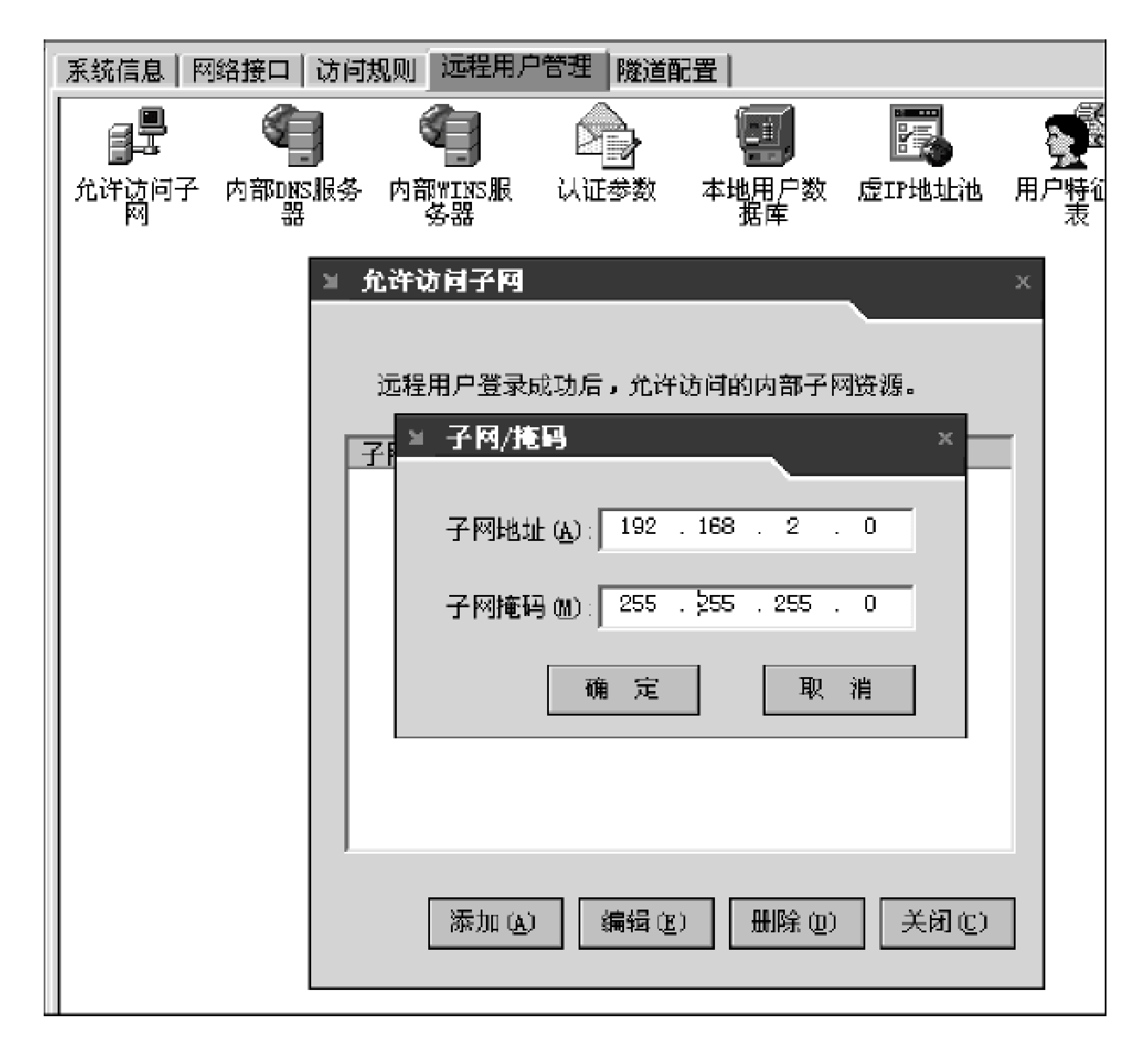


图 2-84 配置“允许访问子网”

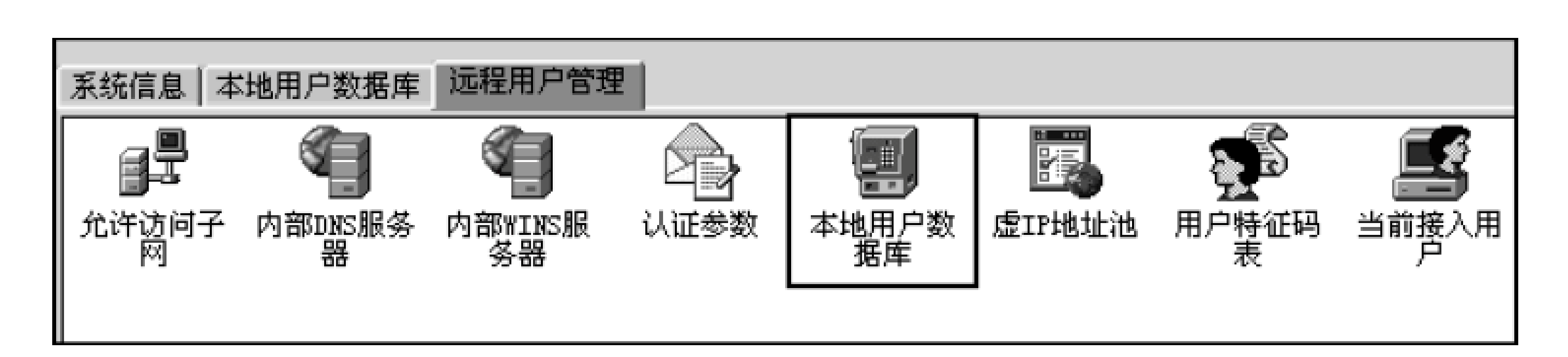


图 2-85 配置本地用户数据库

在打开的“本地用户数据库”管理界面上选择“添加用户”按钮，配置本地数据库中用户信息：用户名、口令和登录权限，操作如图 2-86 所示。

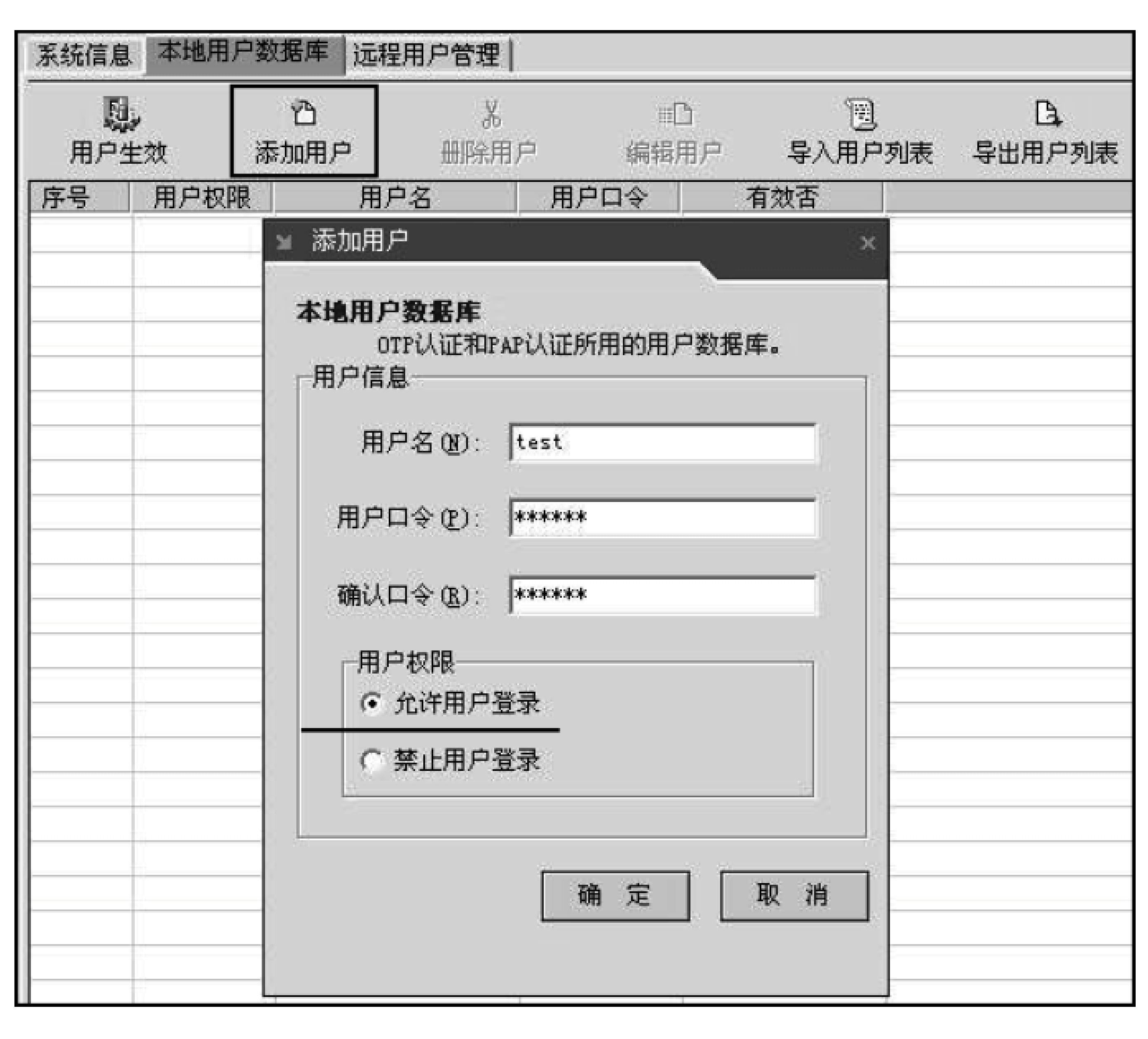


图 2-86 配置本地数据库中用户信息

在图 2-86 所示的“本地用户数据库”界面上单击“用户生效”按钮，让配置的用户信息生效(注意：添加完用户后一定要单击“用户生效”按钮，否则新添加的用户依然不可使用)，如图 2-87、图 2-88 所示。



图 2-87　让配置的用户信息生效(1)



图 2-88　让配置的用户信息生效(2)

(4) 配置“虚 IP 地址池”。

在打开图 2-85“远程用户管理”界面上配置“虚 IP 地址池”信息，如图 2-89 所示。

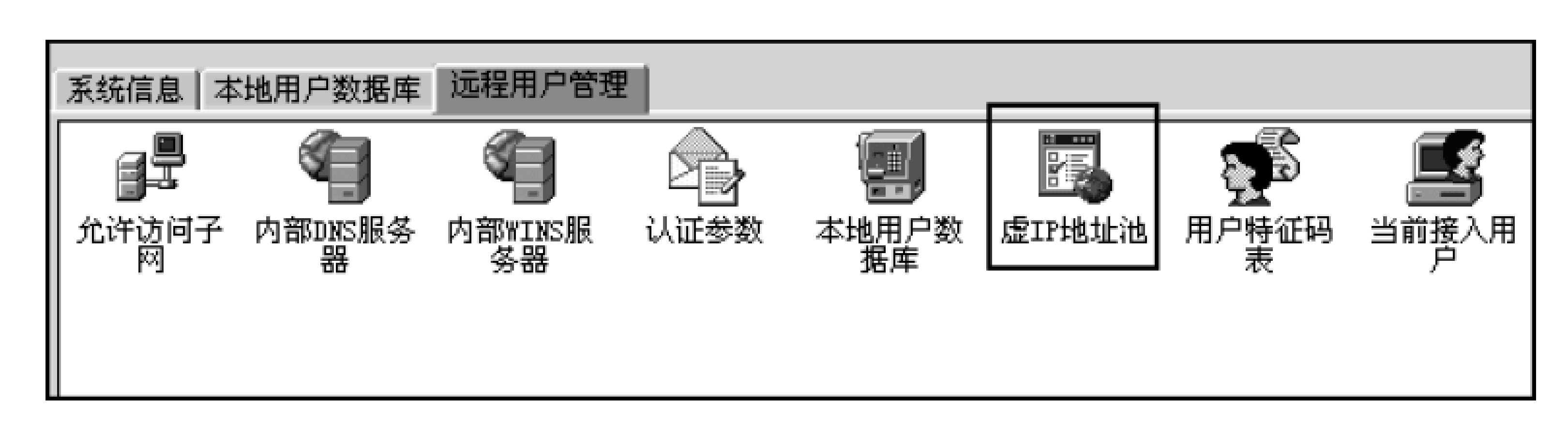


图 2-89　配置“虚 IP 地址池”信息(1)

在打开“虚 IP 地址池”管理界面上选择“添加”、“删除”、“编辑”图标，配置“子网地址、连续地址”信息，如图 2-90 所示。

注意：分配 PC 的虚拟 IP 地址，既可以是定义一个地址池，由 VPN 网关自动分配，也可以是管理员一个 IP 对应一个用户的分配。本实验选择地址池方式，由系统自动分配，并且选择定义“子网地址”的地址池。

虚 IP 是网络管理员分配给远程移动用户的 IP，表示只有拥有该 IP 的 PC 才能获得保密企业网内部的访问权限。因此，管理员设置的虚 IP 一定不要与远程 PC 的 IP，以及网络内部的 IP 发生冲突，否则远程 PC 在和 VPN 网关建立隧道后，因地址冲突的问题，



图 2-90 配置“虚 IP 地址池”信息(2)

也造成无法访问局域网内部的服务器。本实验中虚 IP 地址池选择一个完全没有使用的网段。如图 2-91 所示,在打开“虚 IP 地址池”管理界面上选择“添加”图标,配置子网地址信息。

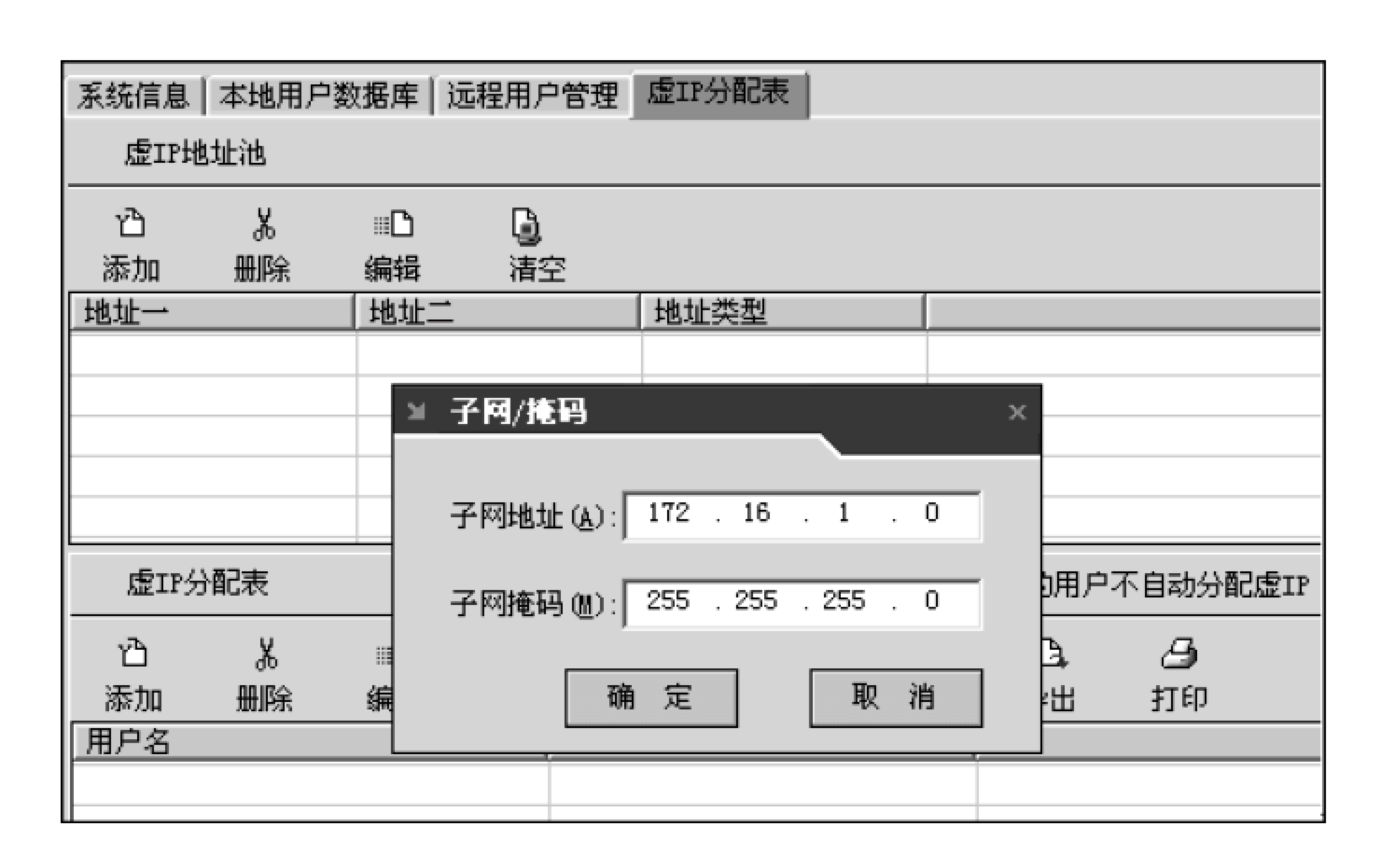


图 2-91 配置添加子网地址信息(1)

如图 2-92 所示,为添加成功的网地址信息。

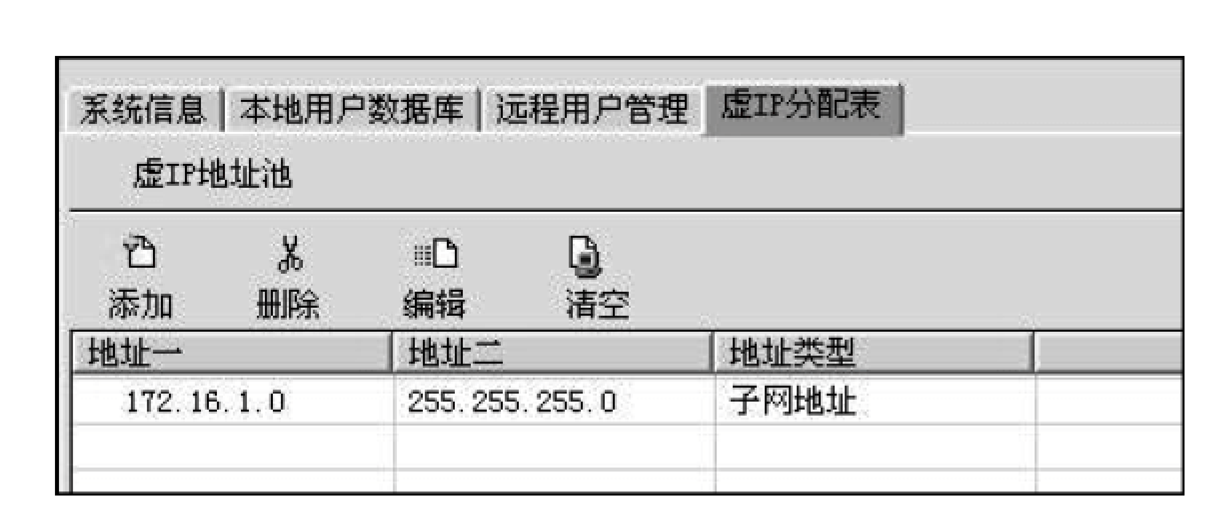


图 2-92 配置添加子网地址信息(2)

(5) 配置“用户特征码表”。

在打开的“远程用户管理”界面上配置“用户特征码表”,如图 2-93 所示。



图 2-93　配置“用户特征码表”信息

打开“用户特征码表”图标，单击“允许接入”单选按钮，分配用户的接入权限，如图 2-94 所示。

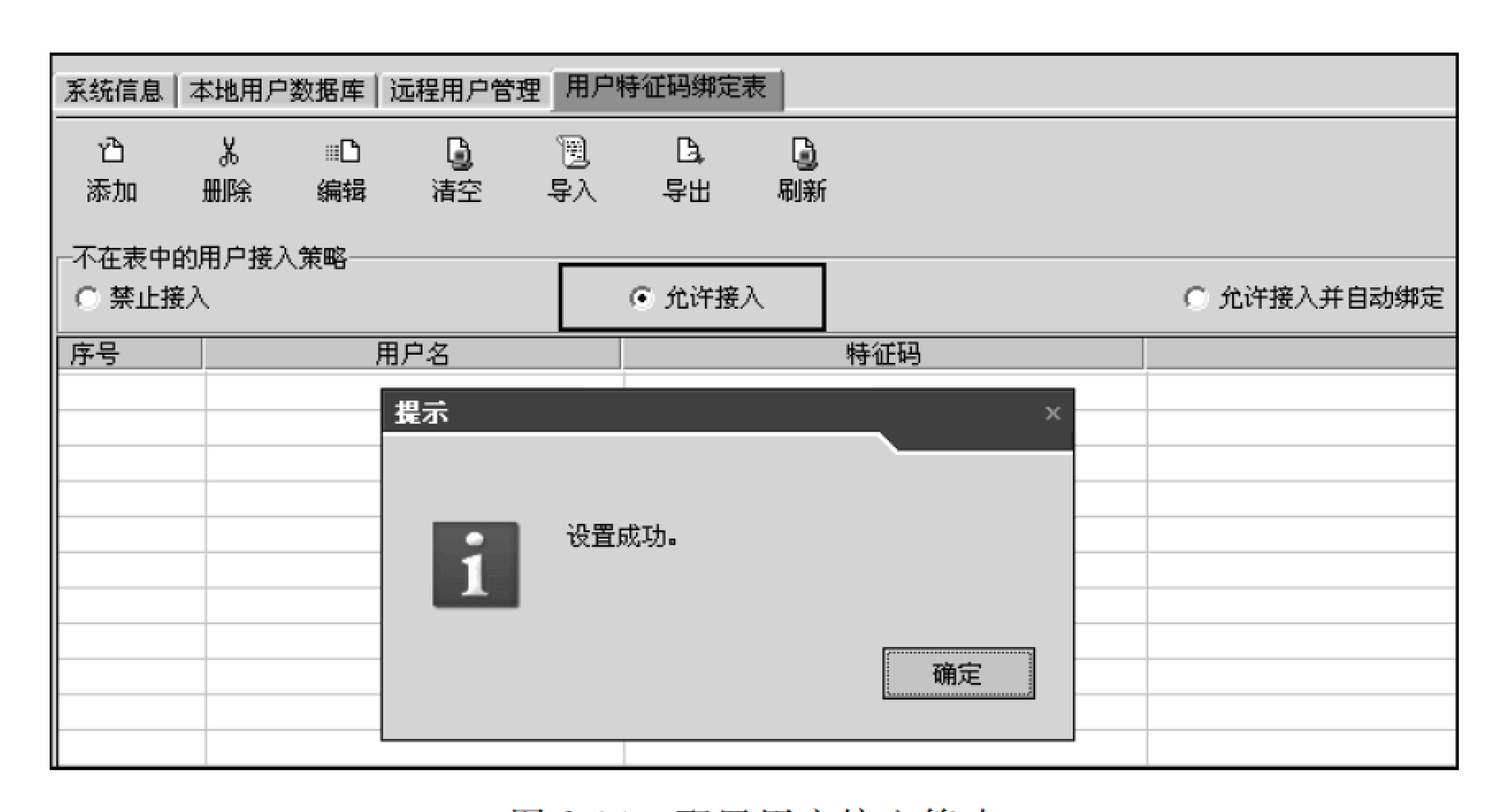


图 2-94　配置用户接入策略

配置说明：“用户特征码表”为需要将远程 PC 的硬件和分配给用户的身份信息绑定需求而设计。如果选择“允许接入并自动绑定”功能，则 VPN 网关会将远程用户的 PC 硬件特征码与该用户的身份认证信息相互绑定，绑定后该用户将无法用自己的身份信息再在其他 PC 设备上建立 VPN 隧道。

本实验中既可以选择“允许接入”，也可以选择“允许接入并自动绑定”。系统默认配置是“禁止接入”。图 2-94 所示选择的是“允许接入”，这表示该用户的身份信息不会和其使用的 PC 硬件绑定。此次实验，“远程用户管理”界面的其他配置项，例如，“内部 DNS 服务器”、“内部 WINS 服务器”、“认证参数”，用户可以根据实际需要选择设置。但本实验因为不涉及这些应用，故不需要进行设置。

第四步：配置防火墙规则。

(1) 定义对象。

① 定义 IP 地址。登录 VPN 网关的管理界面，在 VPN 管理软件主界面上，选择左侧树形列表菜单，进入“防火墙”→“对象管理”→“IP 地址对象”界面，如图 2-95 所示。

打开“IP 地址对象”后，出现“对象配置”管理界面，选择“添加对象”按钮，在打开的对话框中：命名为“出差人员”对象名称，如图 2-96 所示。

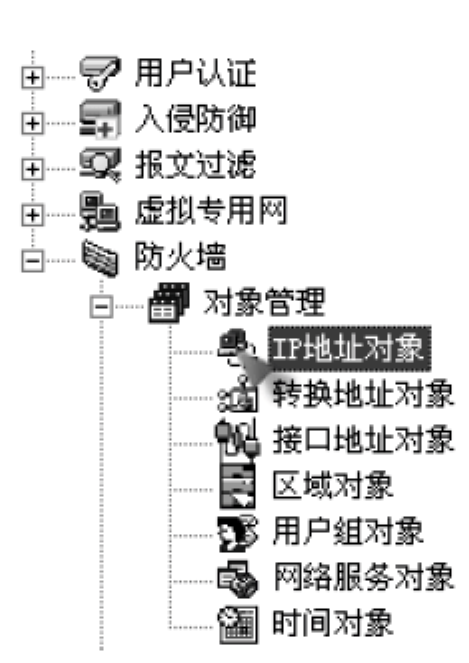


图 2-95　定义 IP 地址对象

添加 IP 地址管理对象名称后，单击“添加成员”按钮，定义“出差人员”的 IP 地址，如图 2-97 所示。

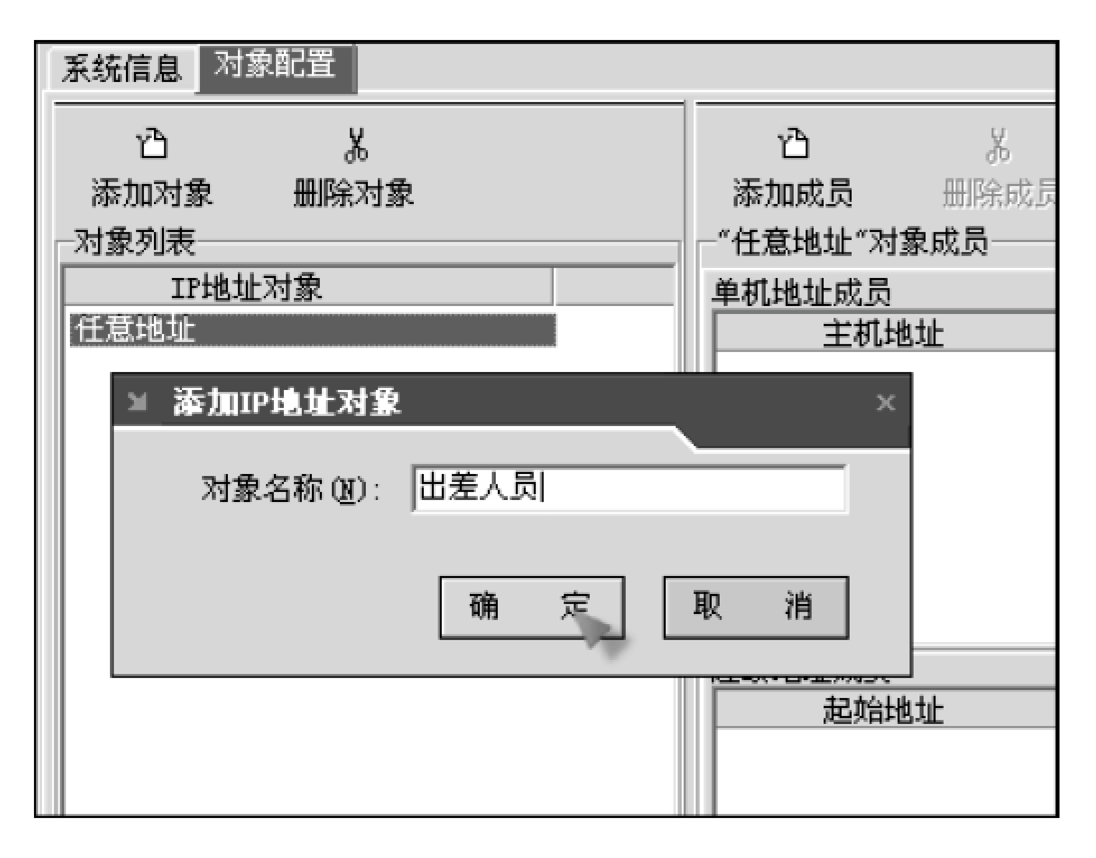


图 2-96 添加 IP 地址管理对象名称

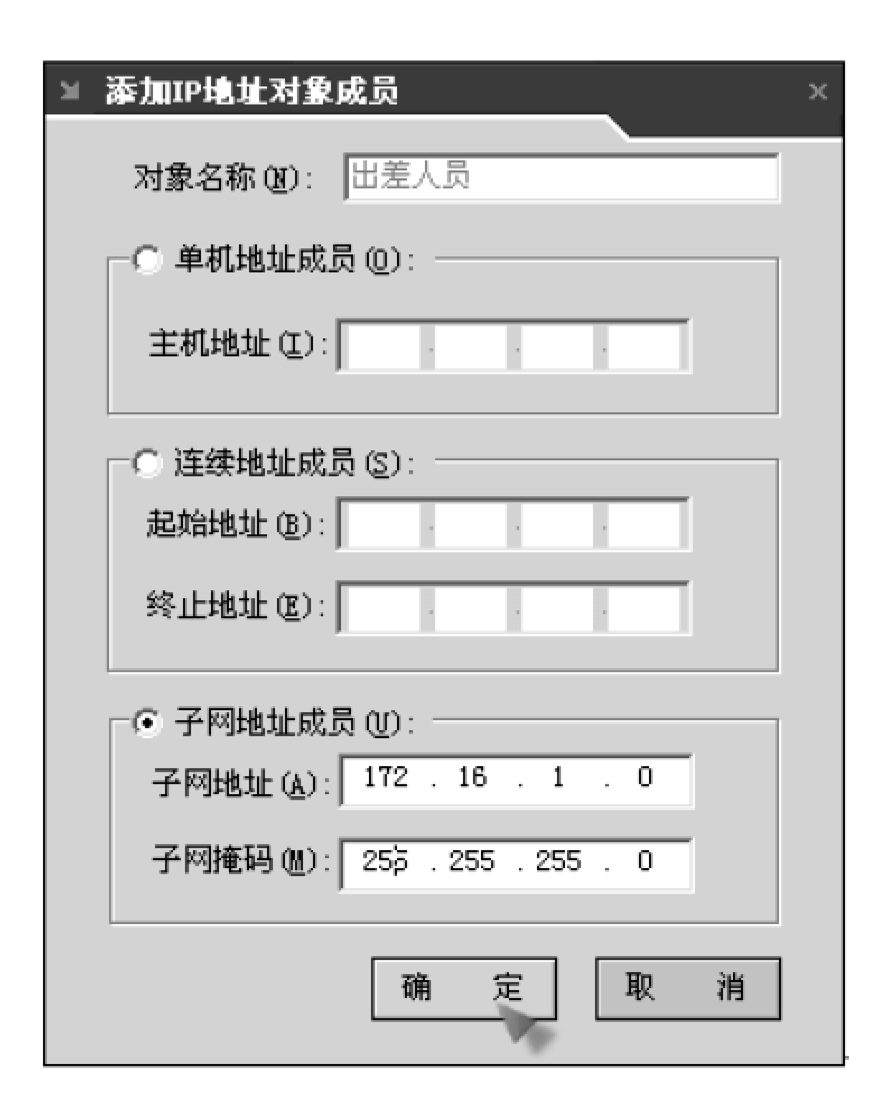


图 2-97 定义出差人员的 IP 地址

继续打开“对象配置”界面，单击“添加对象”按钮，在打开的对话框中命名为“服务器”对象名称，如图 2-98 所示。

添加 IP 地址管理对象名称后，单击“添加成员”按钮，定义“服务器”对象的 IP 地址，如图 2-99 所示。



图 2-98 继续添加 IP 地址管理对象名称



图 2-99 定义服务器对象的 IP 地址

② 定义网络服务对象。在 VPN 管理软件主界面上，选择左侧树形列表菜单，进入“防火墙”→“对象管理”→“网络服务对象”界面，如图 2-100 所示。

在启动“对象配置” 界面中，可以自行对具体的网络服务进行定义；在这里使用系统默认的“常用服务”，如图 2-101 所示。

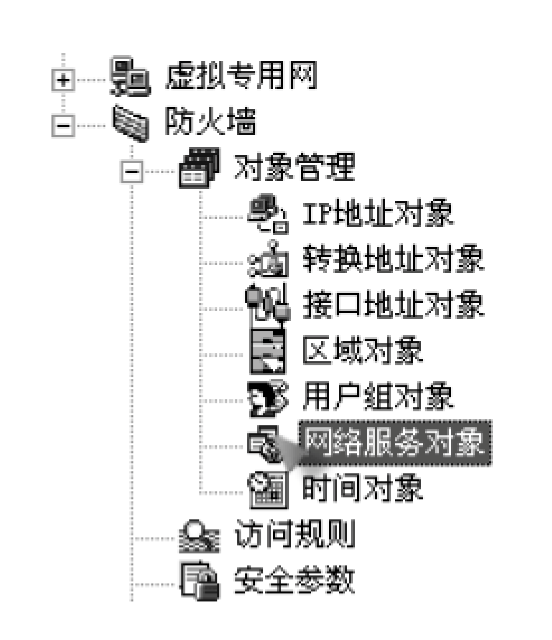


图 2-100　定义网络服务对象

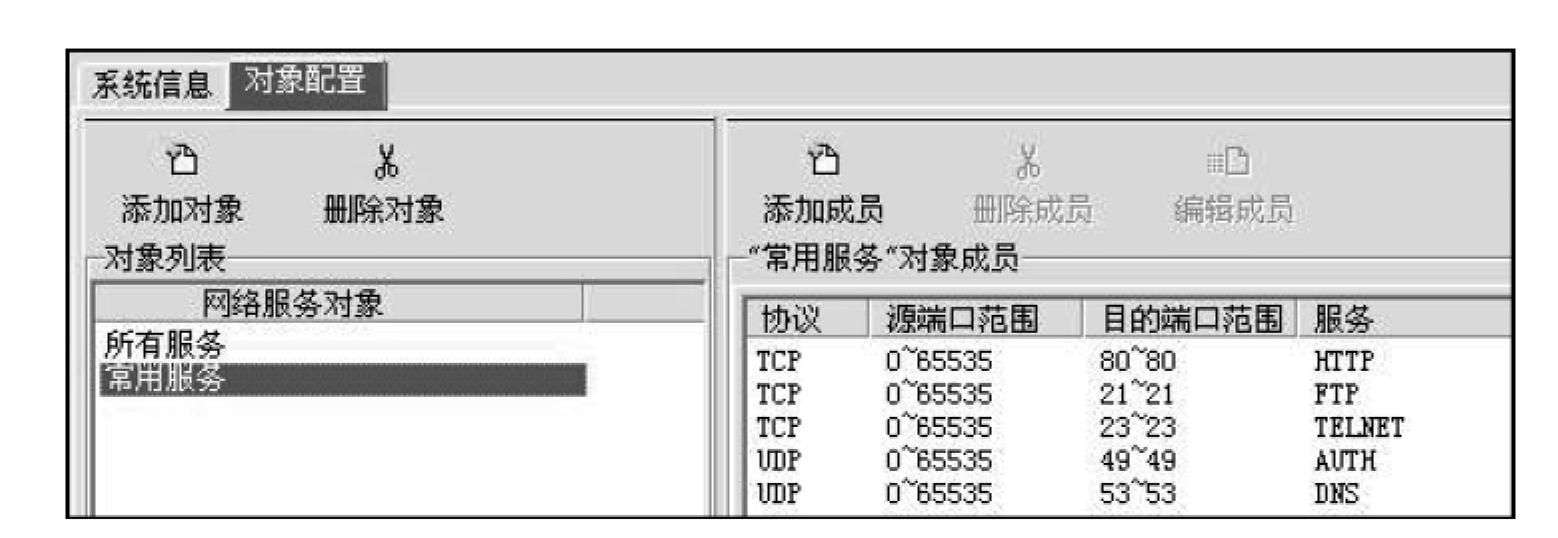


图 2-101　定义服务对象常用服务功能

③ 定义时间对象。在 VPN 管理软件主界面上，选择左侧树形列表菜单，选择进入“防火墙”→“对象管理”→“时间对象”界面，如图 2-102 所示。

在启动“对象配置” 界面中，在“时间对象”一栏，默认的有如下三种时间对象，也可以自行定义其他一些时间段，如图 2-103～图 2-105 所示。

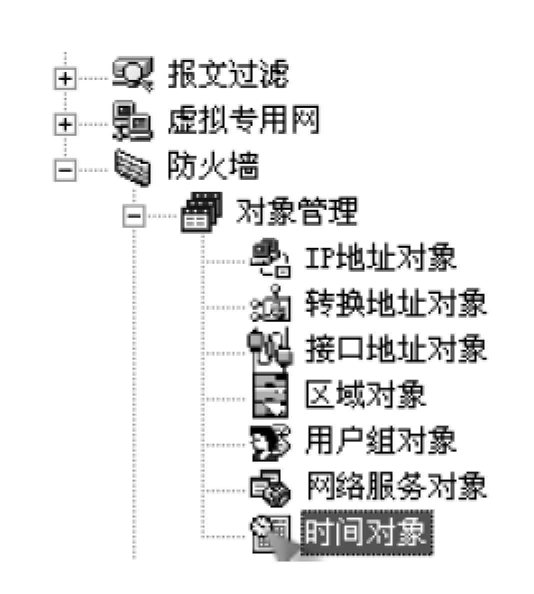


图 2-102　定义时间对象

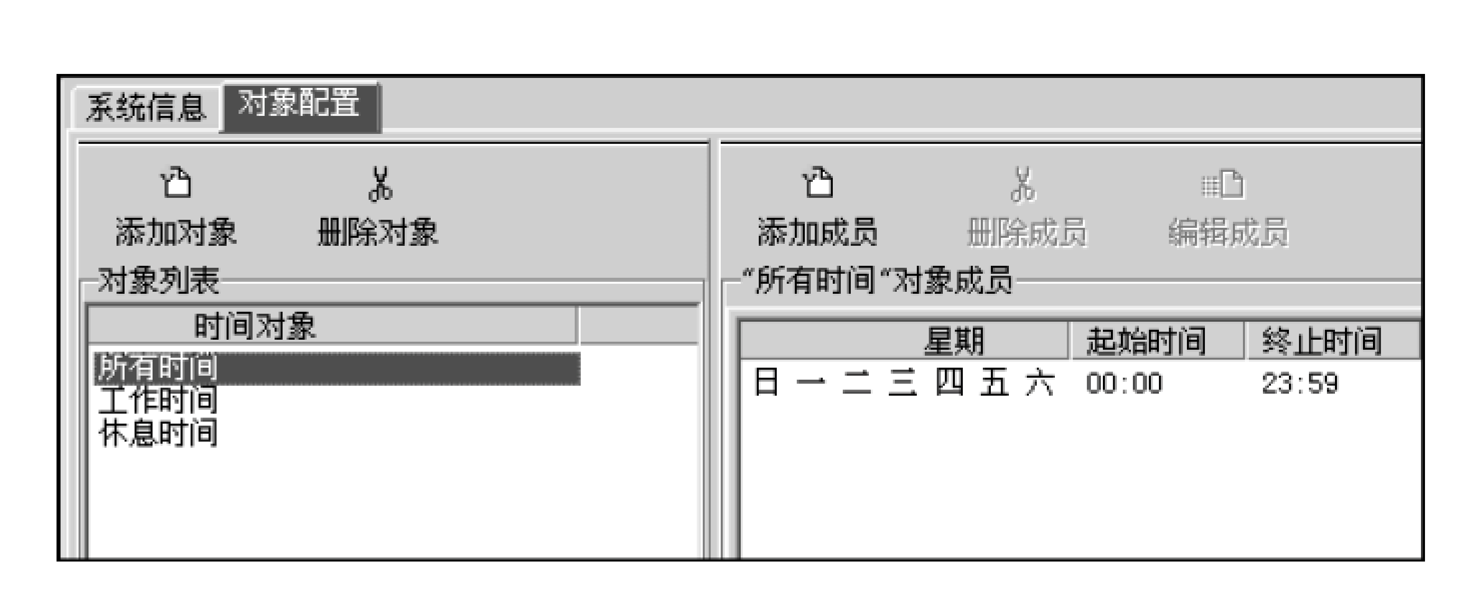


图 2-103　默认所有三种时间对象

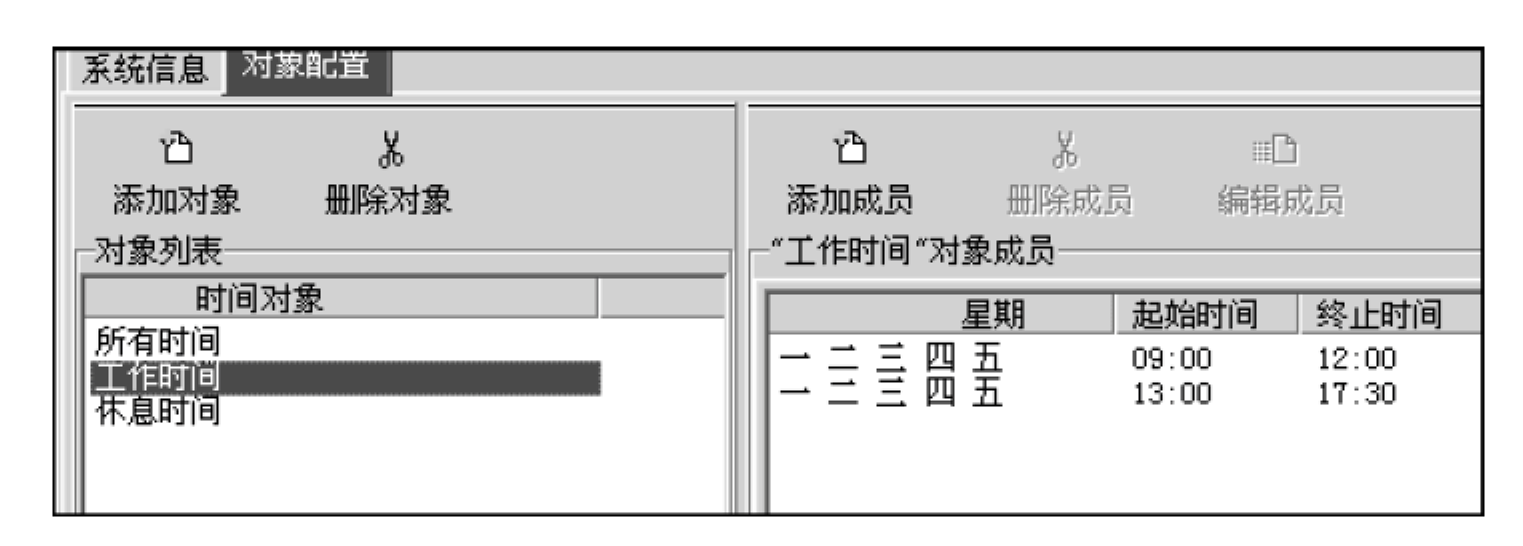


图 2-104　默认工作时间对象

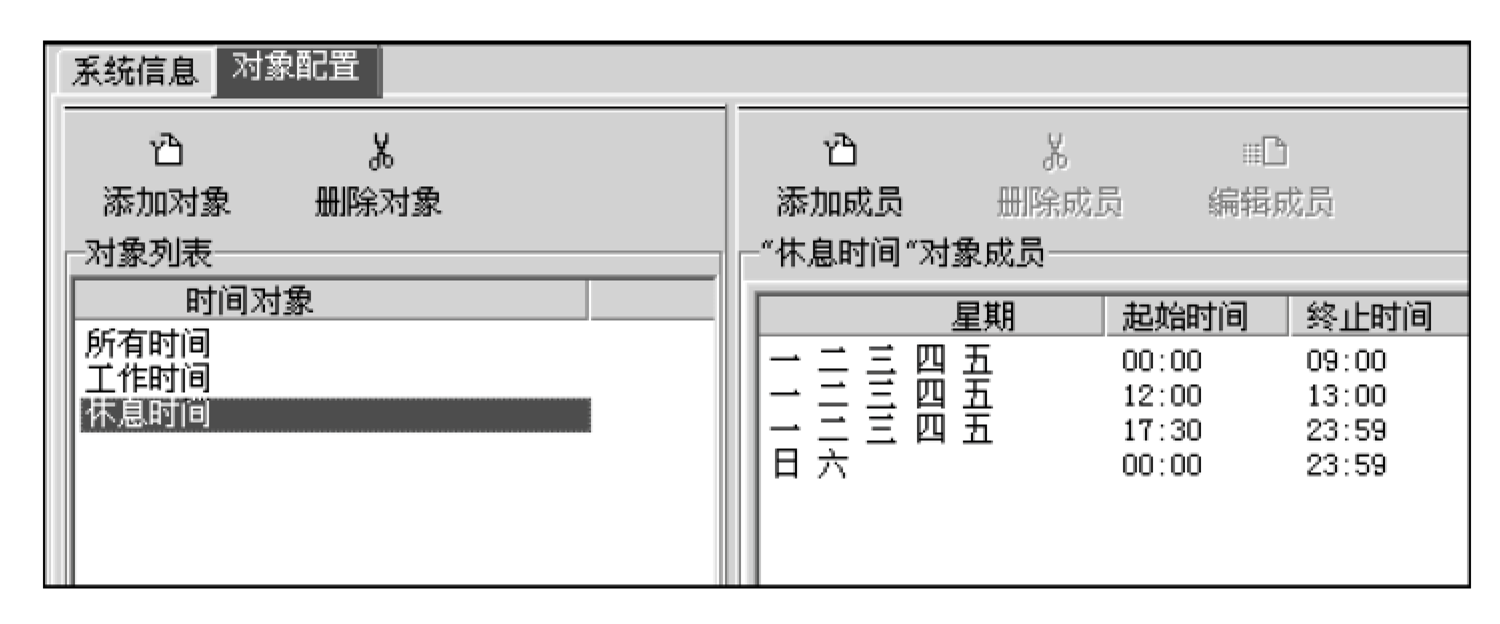


图 2-105　默认休息时间对象

(2) 定义规则。

做好以上对象定义以后，就可以进入规则定义界面。

在 VPN 管理软件主界面上打开左侧树形列表菜单，选择"防火墙"→"访问规则"界面，如图 2-106 所示。

在打开的"访问规则"界面单击"添加规则"按钮，启动"新建防火墙规则"对话框，定义如图 2-107 所示防火墙规则。

继续打开"访问规则"定义界面，单击"编辑规则"按钮，启动"编辑防火墙规则"对话框，如图 2-108 所示。



图 2-106　进入规则定义的界面



图 2-107　"新建防火墙规则"对话框

在启动的"编辑防火墙规则"对话框显示规则定义窗口，可以分别对"源对象"、"目的对象"、"网络服务"、"工作时间"进行定义。编辑完成防火墙规则后，单击"确定"按钮以后，即可完成规则编辑，如图 2-109 所示。

新添加的规则默认位于规则列表最后一条，而且位于"允许所有"和"拒绝所有"两条规则之后。按照规则列表由上至下匹配的顺序来看，新规则在这样的排列下不会生效，所以，要使规则生效，必须把它移动到最顶端，使其最优先执行，如图 2-110 所示。

以上步骤完成后，防火墙规则定义部分完成。

第五步：配置远程接入客户端。

(1) 第一次运行 RG-SRA 程序后，打开如图 2-111 所示窗口。

(2) 建立一个与 VPN 网关的隧道连接。

在运行 RG-SRA 程序主界面上单击"新建连接"按钮，建立一个与 VPN 网关的隧道连接，如图 2-112 所示。

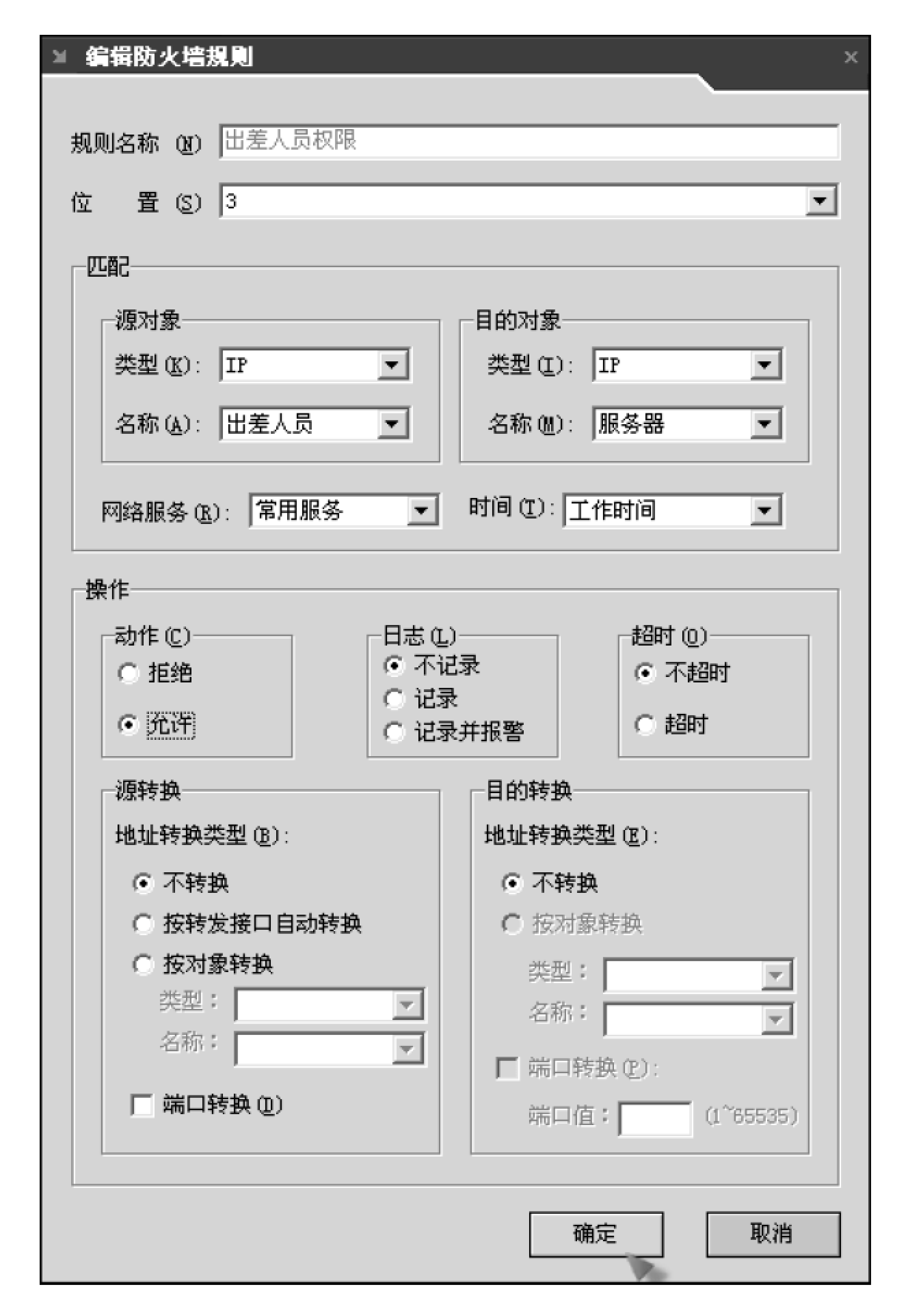


图 2-108　规则定义窗口



图 2-109　完成规则编辑



图 2-110　调整规则检查顺序

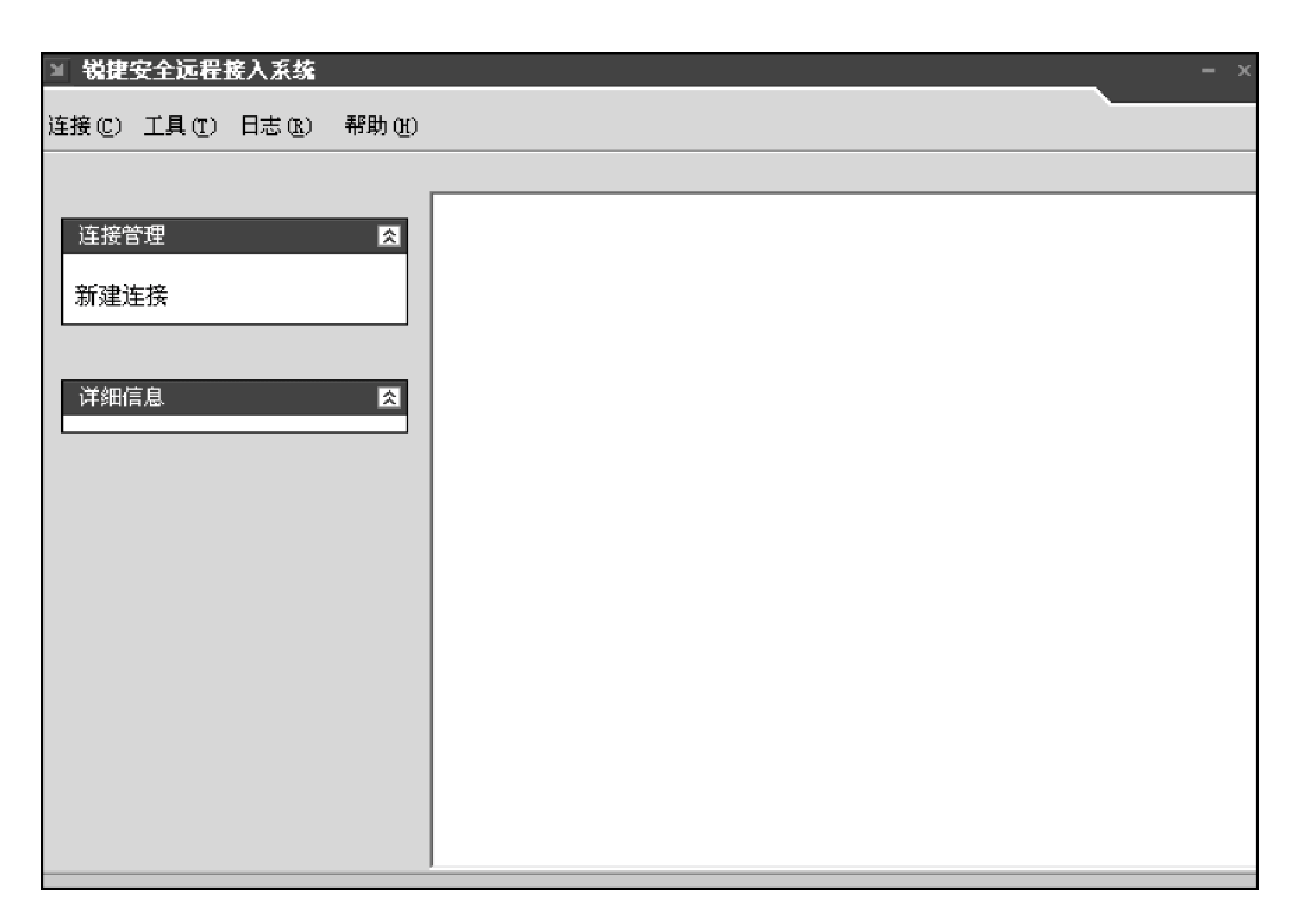


图 2-111 运行 RG-SRA 程序



图 2-112 新建 VPN 网关的隧道连接

在“添加新连接”对话框中，填写新建 VPN 网关的隧道连接的基本信息：连接标示、服务器地址、认证方式等，如图 2-113 所示。

如图 2-114 所示是配置成功“新建 VPN 网关的隧道连接”基本信息。单击“确定”按钮后，显示建立完成的一个与 VPN 网关的隧道连接标号，如图 2-115 所示。

(3) 运行该隧道连接，建立 VPN 隧道。

在运行 RG-SRA 程序主界面上，单击“连接管理”按钮，管理新建立 VPN 网关的隧道

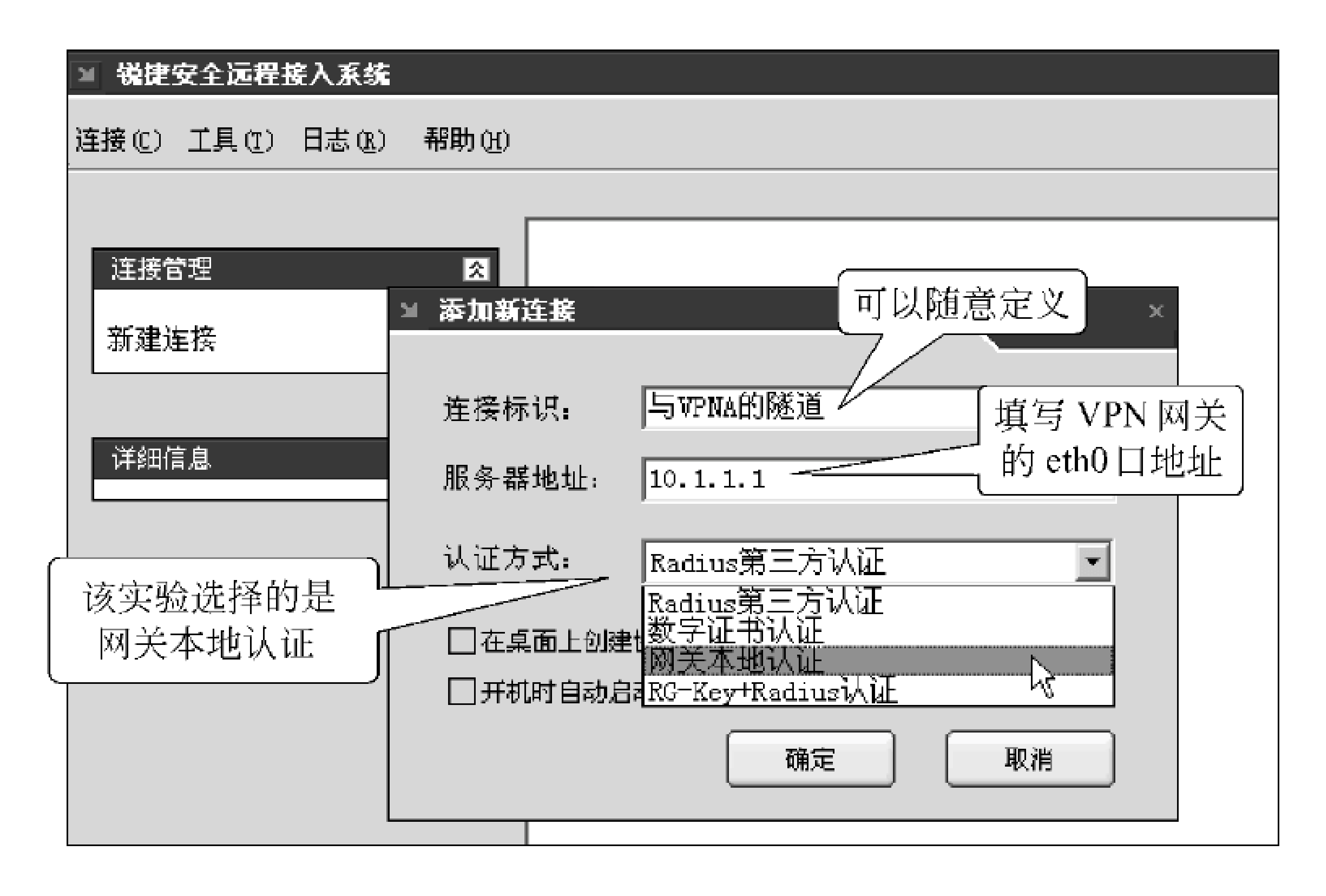


图 2-113　配置新建隧道连接的基本信息(1)

图 2-114　配置新建隧道连接的基本信息(2)

图 2-115　建立完成 VPN 网关的隧道连接

连接，右击打开快捷菜单，选择“启动连接”命令，启动新建的隧道连接，如图 2-116 所示。

通过“启动连接”命令，启动新建的隧道连接后，打开如图 2-117 所示 VPN 连接对话框，输入身份认证所必需的账号、密码，即在 VPN 网关上添加的用户。

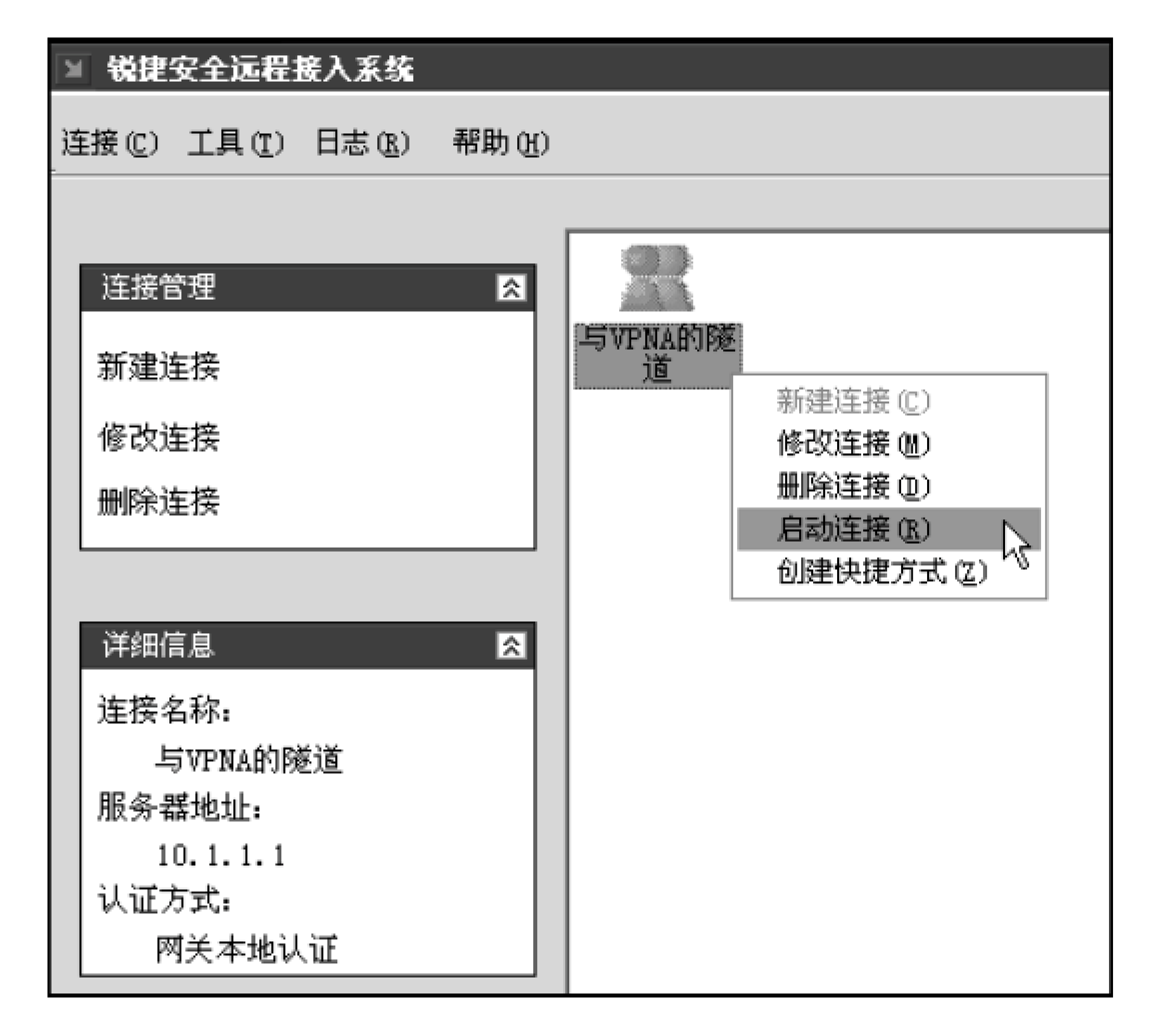


图 2-116　启动新建的隧道连接



图 2-117　登录 VPN 远程安全接入系统

输入身份认证信息后，单击“连接”按钮后，系统自动进行身份认证，并且开始 IKE 协商，如图 2-118 所示。



图 2-118　系统自动进行身份认证

系统自动进行身份认证后，与远程隧道连接建立成功，SRA 程序会自动缩小图标显示在屏幕的右下角，如图 2-119 所示。

选择 SRA 程序运行成功缩小图标，右击打开快捷菜单，在菜单中选择“详细配置”命令，可以查看到隧道信息，如图 2-120 所示。



图 2-119　SRA 程序运行成功缩小图标



图 2-120　查看到隧道信息

如图 2-121 所示信息为查看到的隧道信息，显示“可访问”表示隧道已建立成功，如果是“不可访问”则表示隧道没有建立成功。“资源信息”中显示的“虚拟 IP 地址”信息，表示该 IP 为 VPN 网关从虚地址池中自动分配给该 PC 的虚 IP。

第六步：验证测试。

在 VPN 网关的管理界面也可看到已经建立成功的隧道信息。

隧道启动后可以在“隧道协商状态”栏目下看到隧道的协商状态，打开“隧道状态”项，显示“第二阶段协商成功”，如图 2-122 所示。

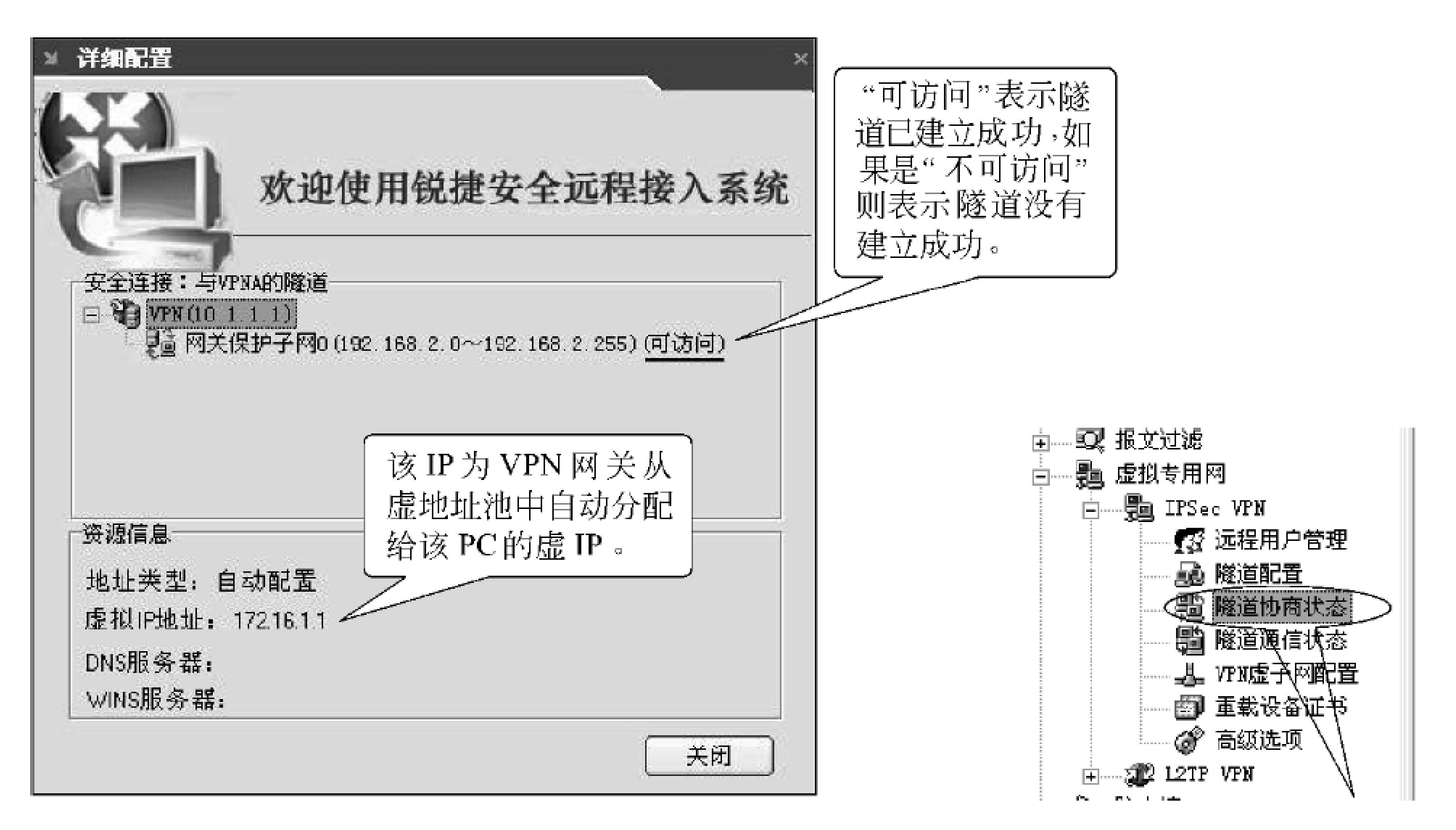


图 2-121　显示隧道配置信息内容　　　　图 2-122　查看隧道协商信息(1)

隧道启动后可以在“隧道协商状态”栏下看到隧道协商状态，“隧道状态”显示“第二阶段协商成功”。VPN 隧道通信情况可以在“隧道协商状态”中查看，如图 2-123 所示。

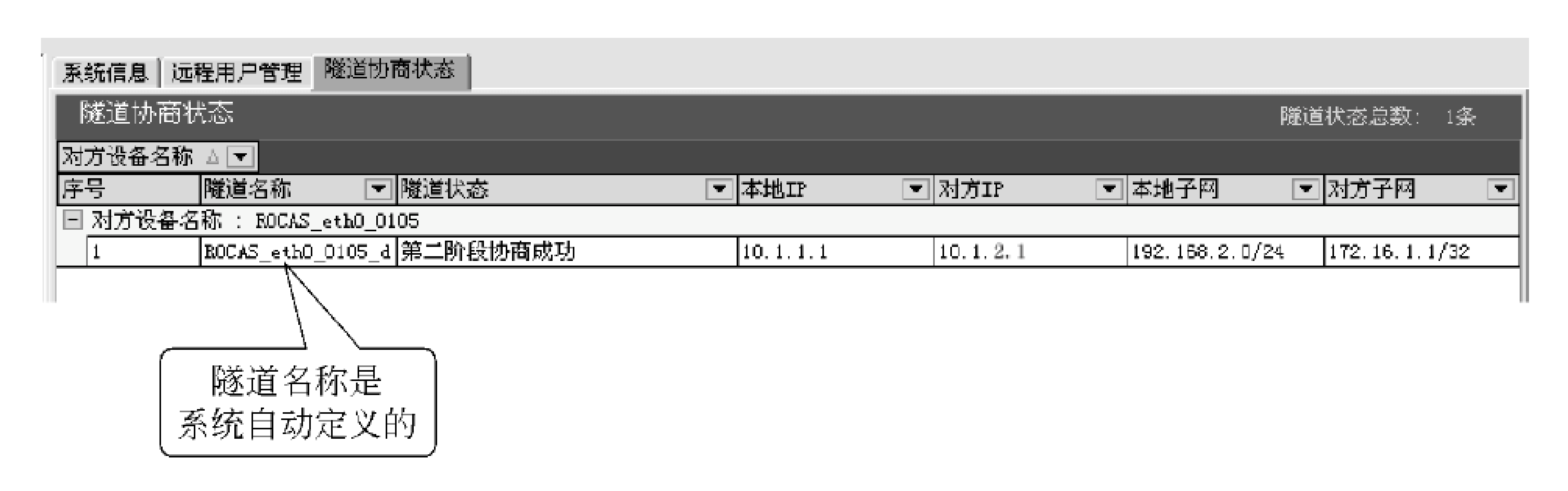


图 2-123　查看隧道协商信息(2)

第七步：进行隧道通信。

在远程用户 PC 上访问服务器提供的服务可以成功，或者在 PC 上 ping 服务器的 IP 地址，可以 ping 通(没有 VPN 隧道前 ping 会失败)。但是由于之前配置了访问规则，所以远程用户 PC 将不能访问公司内部网络的其他主机和服务，只能访问地址为 192.168.2.2 的服务器。VPN 隧道的通信情况可以在“隧道通信状态”中查看到，如图 2-124 所示。

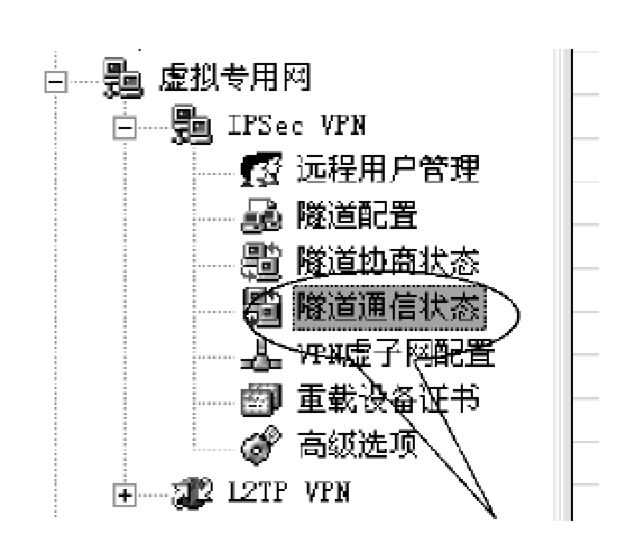


图 2-124　查看隧道通信信息(1)

隧道启动后,可以在"隧道通信状态"栏下看到隧道的通信状态,打开"隧道通信状态"可以显示"第二阶段协商成功"对话框。VPN 隧道的通信情况可以在"隧道通信状态"中查看到,如图 2-125 所示。

系统信息 | 网络接口 | 隧道配置 | 隧道通信状态 | 隧道协商状态

隧道通信状态

序号	类型	本地子网	对方子网	发送成功包数	发送失败包数	发送成功字节数
1	IKE	192.168.1.0/24	192.168.2.0/24	14	0	840

图 2-125　查看隧道通信信息(2)

【注意事项】

- 实验环境地址可以随意定义,但请不要使用 1.1.1.0 这个网段的 IP,因为某些功能实现的需要,VPN 系统内部已占用该网段的部分 IP。
- 该实验中,VPN 网关的防火墙规则为全部开放。但在实际的网络环境中,如果 VPN 网关直接连接 Internet 网络,则一定需要启用防火墙规则。
- RG-SRA 是 VPN 客户端软件程序,如果 PC 机上已预装其他厂家的 VPN 客户端程序,请先卸载其他厂家的 VPN 客户端程序,否则可能 RG-SRA 无法正常工作。
- RG-SRA 作为安全产品,安装后会对系统的网卡、端口、协议等方面有改动,因此会和部分防火墙或者防病毒程序不兼容。推荐用户使用没有安装任何第三方防火墙、防病毒程序的机器来做实验。

第 3 章 VPN 专用设备 Site-to-Site 的安全

3.1 构建站点到站点 IPSec VPN(预共享密钥)

【实验名称】

构建站点到站点 IPSec VPN(预共享密钥)。

【实验目的】

学习配置站点到站点(Site-to-Site)的 IPSec VPN 隧道,加深对 IPSec 的理解。

【背景描述】

北京的某公司在上海设立分公司,分公司要远程访问总公司内网中的各种网络资源,例如,CRM 系统、FTP 服务器等。由于在 Internet 上传输数据本身存在安全隐患,公司希望通过 IPSec VPN 技术实现数据的安全传输。

【需求分析】

需求:解决上海分公司和北京总公司之间通过 Internet 进行数据传输的安全问题。

分析:IPSec VPN 技术通过隧道技术、加解密技术、密钥管理技术、认证技术等有效地保证了数据在 Internet 传输的安全性,是目前最安全、使用最广泛的 VPN 技术。通过建立 IPSec VPN 的加密隧道,实现分公司和总公司之间的安全的数据传输。

【实验拓扑】

如图 3-1 所示网络拓扑,是某公司为解决上海分公司和北京总公司之间通过 Internet 进行数据传输的安全问题。分公司要远程访问总公司内网中的各种网络资源,需要在 Internet 上传输数据,公司希望通过配置站点到站点(Site-to-Site)的 IPSec VPN 隧道技术,实现数据在 Internet 上的安全传输。

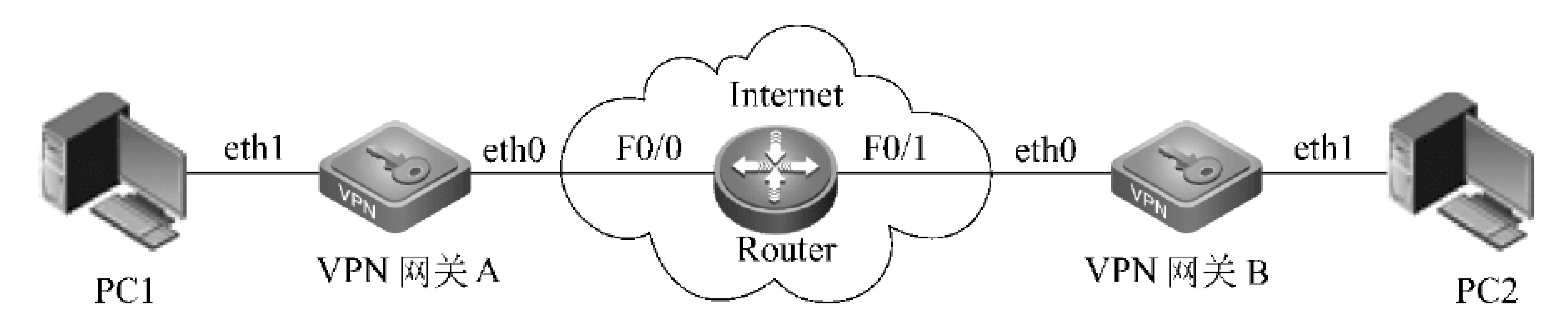


图 3-1　构建站点到站点 IPSec VPN

【实验设备】

RG-WALL VPN 网关：2 台；PC：2 台；路由器：1 台。

【预备知识】

IKE 工作原理

IPSec 协议是基于 IP 网络(包括 Intranet、Extranet 和 Internet)，由 IETF 正式定制的开放的 IP 安全标准，IPSec 提供三种不同的形式保护通过公有或私有 IP 网络传送数据的安全性。

- 认证：作用是确定所接收的数据与所发送数据的一致性，同时确定申请发送者在实际发送中的真实身份。
- 数据完整：作用是保证数据从源发地到目的地的传送过程中，没有任何不可检测的数据丢失与改变。
- 机密性：作用是使相应的接收者能获取发送的真正内容，无意获取数据的接收者无法获知数据的真正内容。

IPSec 协议由三个基本要素来提供以上三种保护形式：认证协议头(AH)、安全加载封装(ESP)和互联网密匙管理协议(IKMP)。认证协议头和安全加载封装可以通过分开或组合使用来达到所希望的保护等级。认证协议头(AH)是在所有数据包头加入一个密码。安全加载封装(ESP)通过对数据包的全部数据和加载内容进行全加密来严格保证传输信息的机密性，这样可以避免其他用户通过监听来打开信息内容，保证只有受信任的用户拥有密匙才能打开内容。

IPSec 协议提供的安全服务，需要使用共享密钥来保证数据验证以及数据的机密性。如果采用人工增加密钥的方法，也可实现基本 IPSec 协议间的互通性，但其在使用上难以扩展。因此需要定义一种标准的方法，用以动态地验证 IPSec 参与各方的身份、协商安全服务以及生成共享密钥等，这种密钥管理协议称为“Internet 密钥交换”(Internet Key Exchange，IKE)。Internet 密钥交换协议是用于交换和管理在 VPN 中使用的加密密钥，协商 AH 和 ESP 协议所使用的密码算法，使用了 UPD 协议来交换密钥和其他安全信息，并将算法所需的密钥放在合适的位置。

IPSec 提供的安全服务，当应用环境规模较小时，可以用手工配置；当应用环境规模较大、参与的节点位置不固定时，IKE 可自动地为参与通信的实体协商，并对安全关联库维护，保障通信安全。

IKE 协议属于一种混合型协议，由 Internet 安全关联、密钥管理协议(ISAKMP)和两种密钥交换协议(OAKLEY 与 SKEME)组成。IKE 创建在由 ISAKMP 定义的框架上，沿用了 OAKLEY 的密钥交换模式以及 SKEME 的共享和密钥更新技术，定义了自己的两种密钥交换方式。

为确保通过 Internet 网使用 IPSec 协议安全通信，Internet 密钥交换 IKE 协议将执行双阶段协商工作。IKE 使用了两个阶段的 ISAKMP 密钥管理协议：第一阶段，协商创建一个通信信道(IKE SA)，并对该信道进行验证，为双方进一步的 IKE 通信提供机密性、消息完整性以及消息源验证服务；第二阶段，使用已建立的 IKE SA 建立 IPSec SA。

IKE 共定义两种交换。第一阶段有两种模式交换：对身份进行保护"主模式"交换以及根据基本 ISAKMP 文档制订"野蛮模式"交换。第二阶段交换使用"快速模式"交换。IKE 定义了两种信息交换：①为通信各方间协商一个 Diffie Hellman 组类型"新组模式"交换；②在 IKE 通信双方间传送错误及状态消息的 ISAKMP 信息交换。

Internet 密钥交换 IKE 解决了在不安全的网络环境(如 Internet)中安全地建立或更新共享密钥的问题。IKE 是非常通用的协议，不仅可为 IPSec 协议协商安全关联，而且可以为 SNMPv3、RIPv2、OSPFv2 等任何要求保密的协议协商安全参数。

【实验原理】

IPSec 协议的主要作用是为 IP 数据通信提供安全服务。IPSec 不是一个单独协议，它是一套完整的体系框架，包括 AH、ESP 和 IKE 三个协议。IPSec 使用了多种加密算法、散列算法、密钥交换方法等为 IP 数据流提供安全保障，提供数据的机密性、数据的完整性、数据源认证和反重放等安全服务。

IKE 为 IPSec 协议提供安全协商，可以使用两种对等体认证方式：预共享密钥和数字签名(或称数字证书)，本实验使用预共享密钥认证方式。

【实验步骤】

第一步：准备好 PC。

准备好 PC1 和 PC2 后，先在 PC1 和 PC2 上安装 VPN 管理软件。具体的安装步骤不在这里详述，查看 VPN 产品的随机说明书和产品光盘。

第二步：搭建拓扑，配置 IP 地址。

按照如图 3-1 所示拓扑图，搭建实验拓扑，并根据如表 3-1 所示编址方案，配置各设备的 IP 地址。

表 3-1 设备 IP 地址

设　　备	接　　口	地　　址
VPN 网关 A	eth1 接口地址	192.168.1.1
	eth0 接口地址	10.1.1.1
PC1	PC1 的 IP 地址	192.168.1.2
	PC1 网关地址	192.168.1.1
VPN 网关 B	eth1 口地址	192.168.2.1
	eth0 口地址	10.1.2.1
PC2	PC2 的 IP 地址	192.168.2.2
	PC2 网关地址	192.168.2.1
Router	F0/0 地址	10.1.1.2
	F0/1 地址	10.1.2.2

说明：PC 及 Router 地址的配置方式不再详述。

(1) 如图 3-2 所示,在模拟客户机 PC1 的超级终端,转入命令行状态,在命令行下配置 VPN 网关 A 的 eth1 口地址。

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manu
al):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.1.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# _
```

图 3-2　命令行模式配置 VPN 网关 eth1 口地址

(2) 如图 3-3 所示,在模拟客户机 PC1 上,打开 VPN 管理软件,登录 VPN 网关 A,然后配置 eth0 口地址。设置如图 3-4 所示 eth0 口地址。

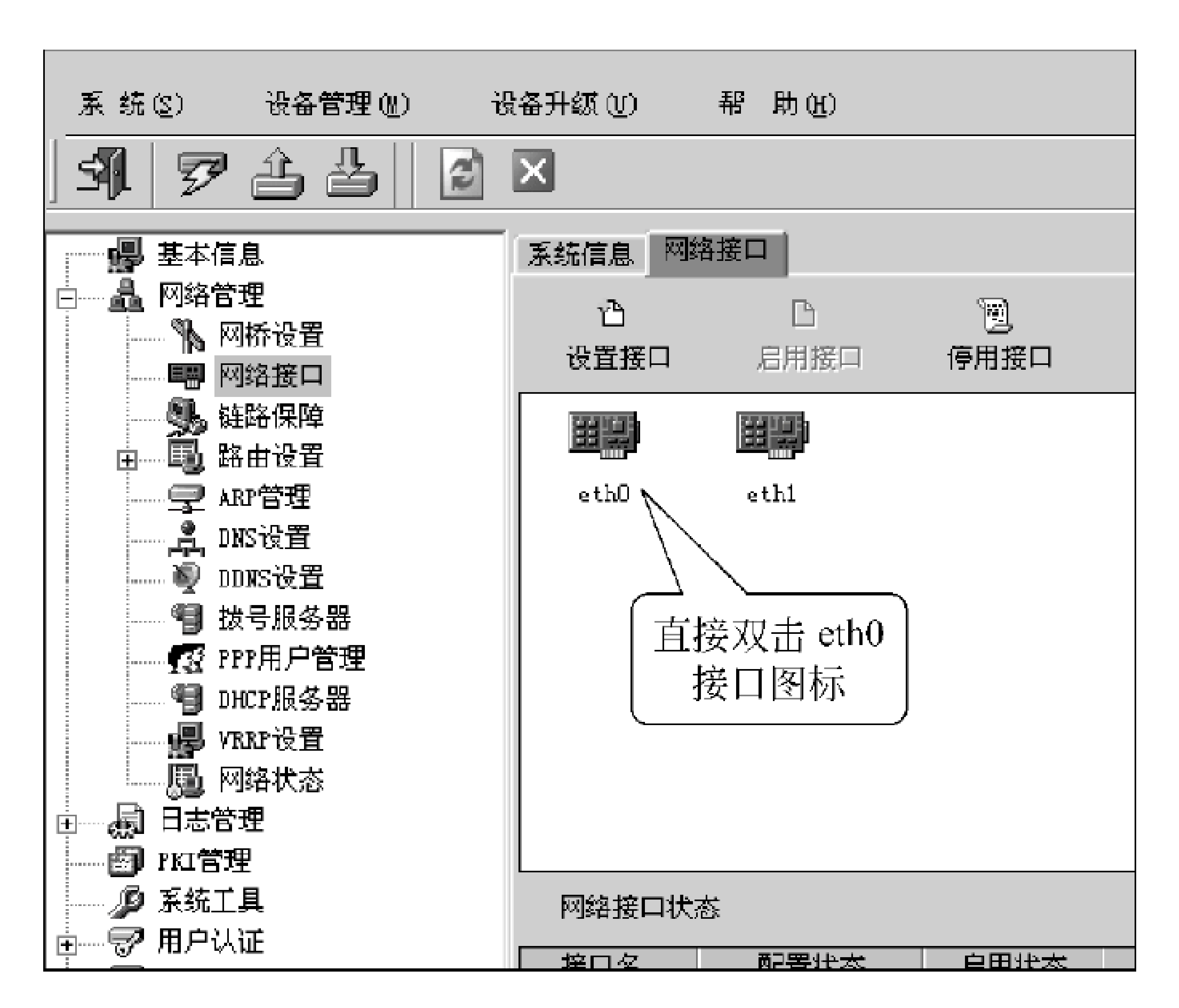


图 3-3　配置 eth0 口地址(1)

(3) 如上过程通过 PC2 的超级终端,在命令行下配置 VPN 网关 B 的 eth1 口地址,如图 3-5 所示。

(4) 通过 PC2 上的 VPN 管理软件登录 VPN 网关 B,然后配置 eth0 口地址,如图 3-6 所示。

设置如图 3-7 所示 eth0 口地址。

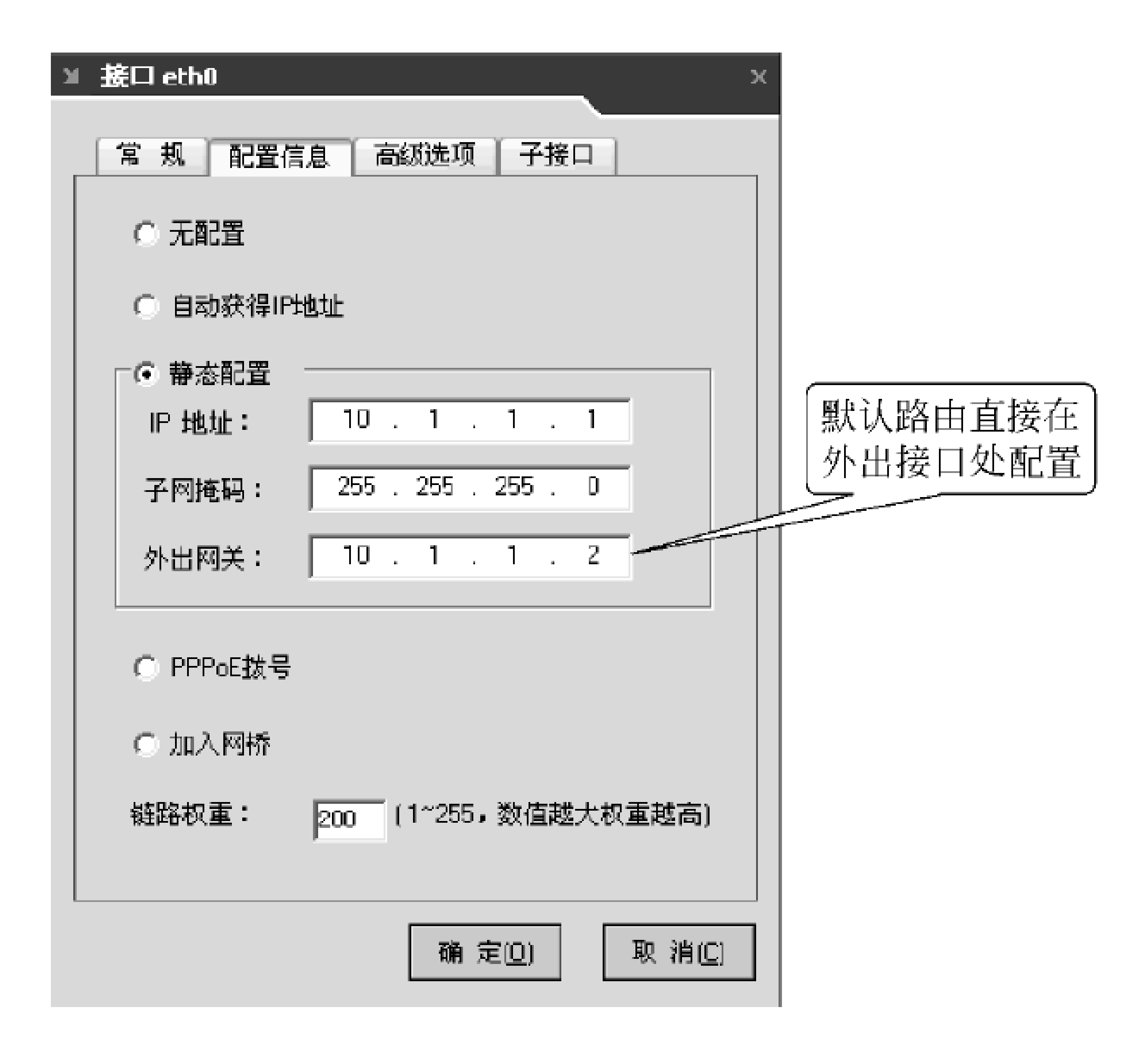


图 3-4　配置 eth0 口地址(2)

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manu
al):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.2.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# _
```

图 3-5　命令行模式配置 VPN 网关 eth1 口地址

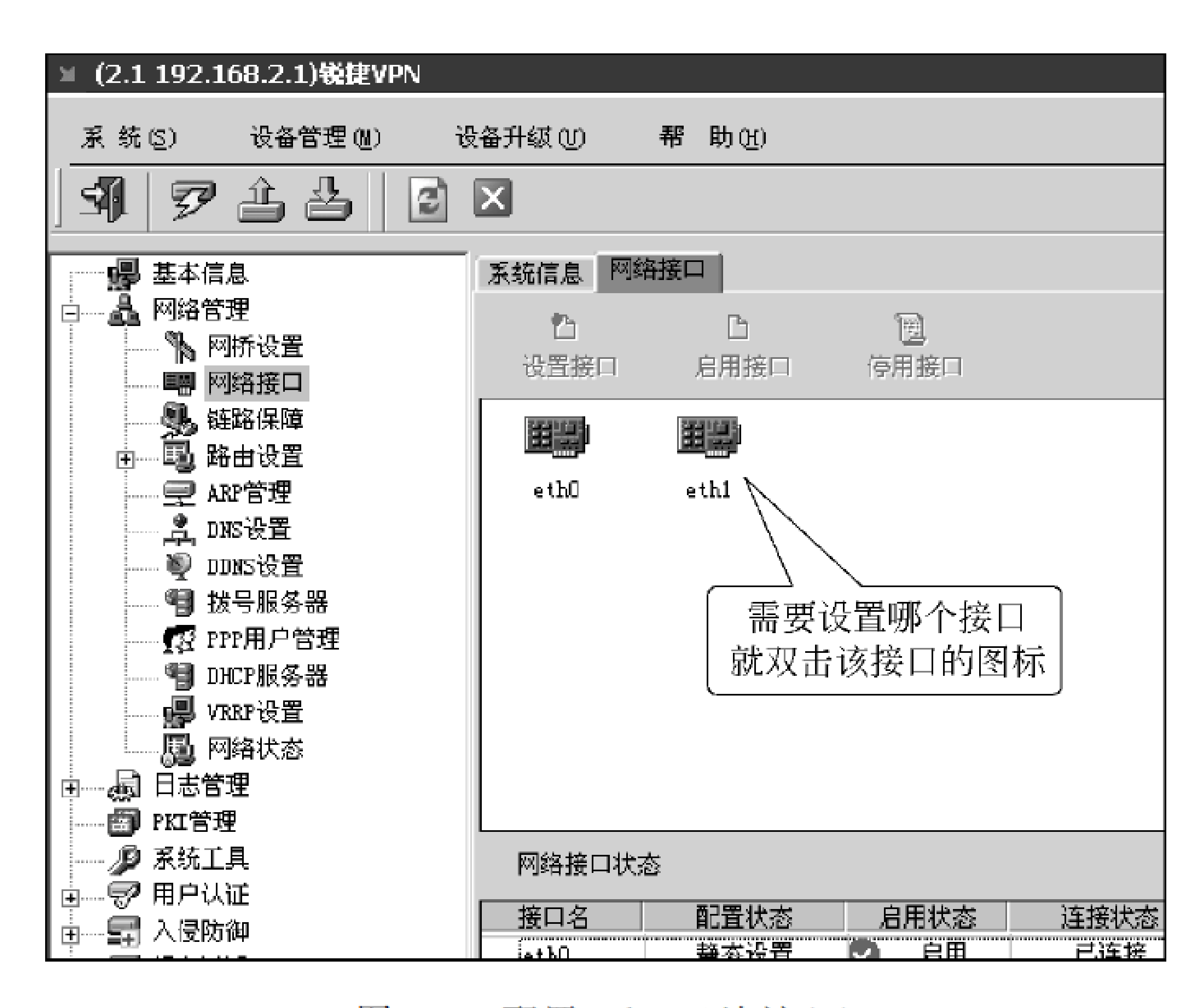


图 3-6　配置 eth0 口地址(1)



图 3-7　配置 eth0 口地址(2)

第三步：配置 VPN 网关 A 的 IPSec VPN 隧道。

(1) 进行设备配置，打开"虚拟专用网"中"隧道配置"项，单击"添加设备"按钮，添加设备，如图 3-8 所示。

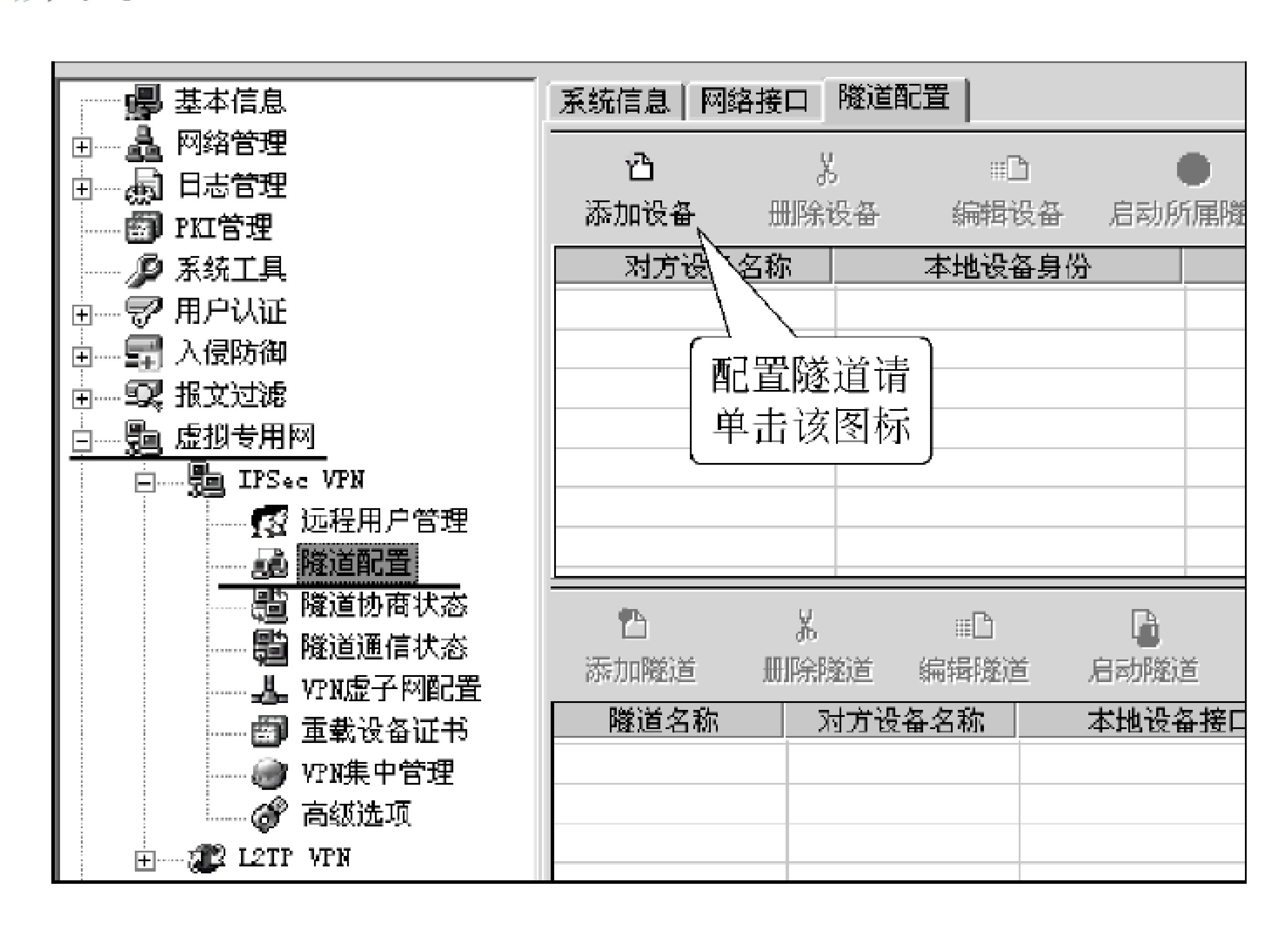


图 3-8　添加 IPSec VPN 隧道设备

在打开的 IPSec VPN 隧道设备配置信息中，选择设备名称和共享密钥，如图 3-9 所示。

如图 3-10 所示，在隧道设备信息的"高级选项"中配置图中设置相关信息。



图 3-9　配置 IPSec VPN 隧道设备信息



图 3-10　配置 IPSec VPN 隧道设备高级选项信息

（2）在“隧道配置”选项中，进行隧道配置，如图 3-11 所示，选择添加的设备，单击“添加隧道”按钮。

如图 3-12 所示，在添加的新隧道中，为添加隧道配置隧道信息。

为添加的信息隧道配置“通信策略”信息，如图 3-13 所示。

添加完隧道后的信息如图 3-14 所示。

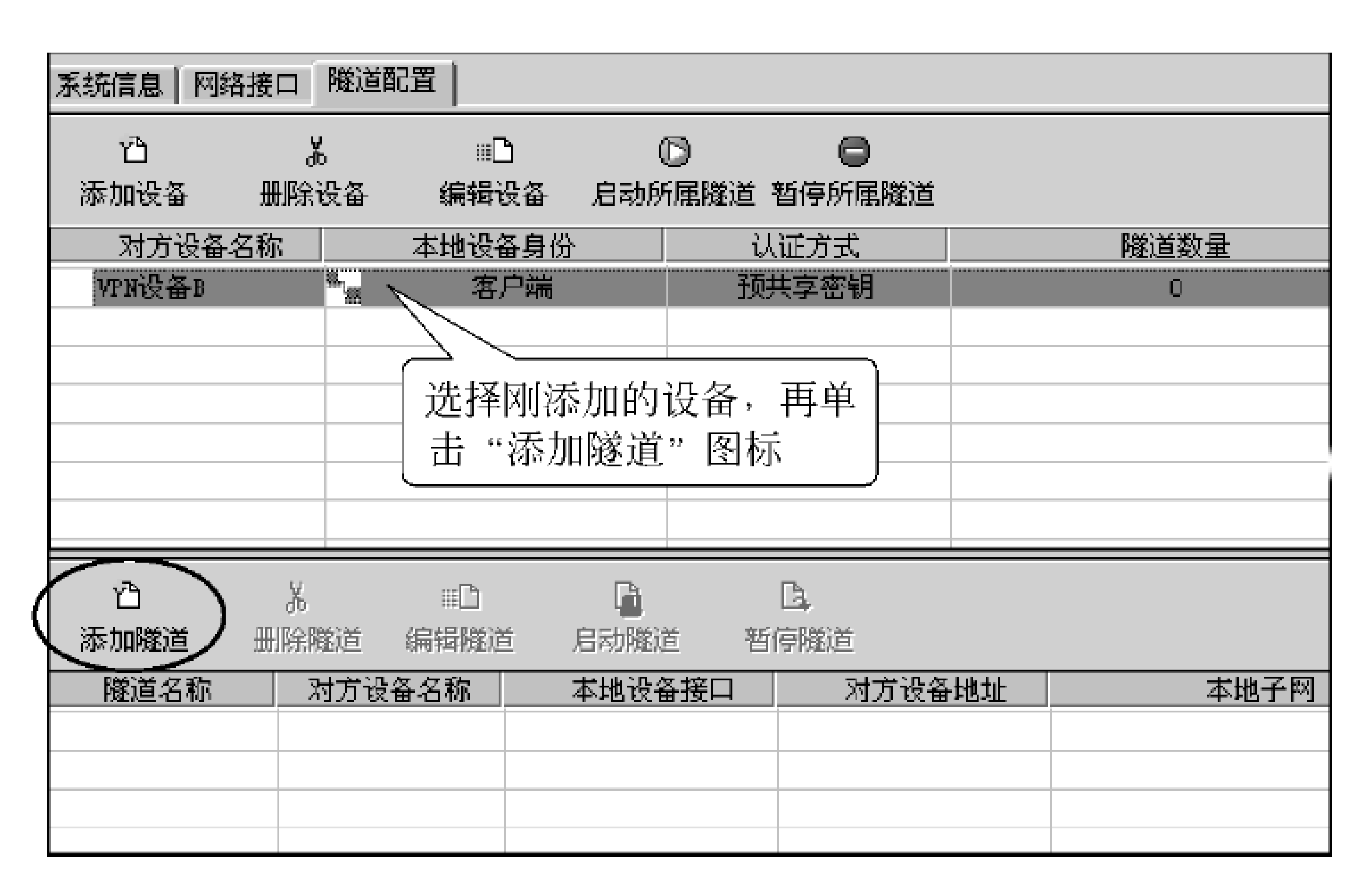


图 3-11　添加新隧道

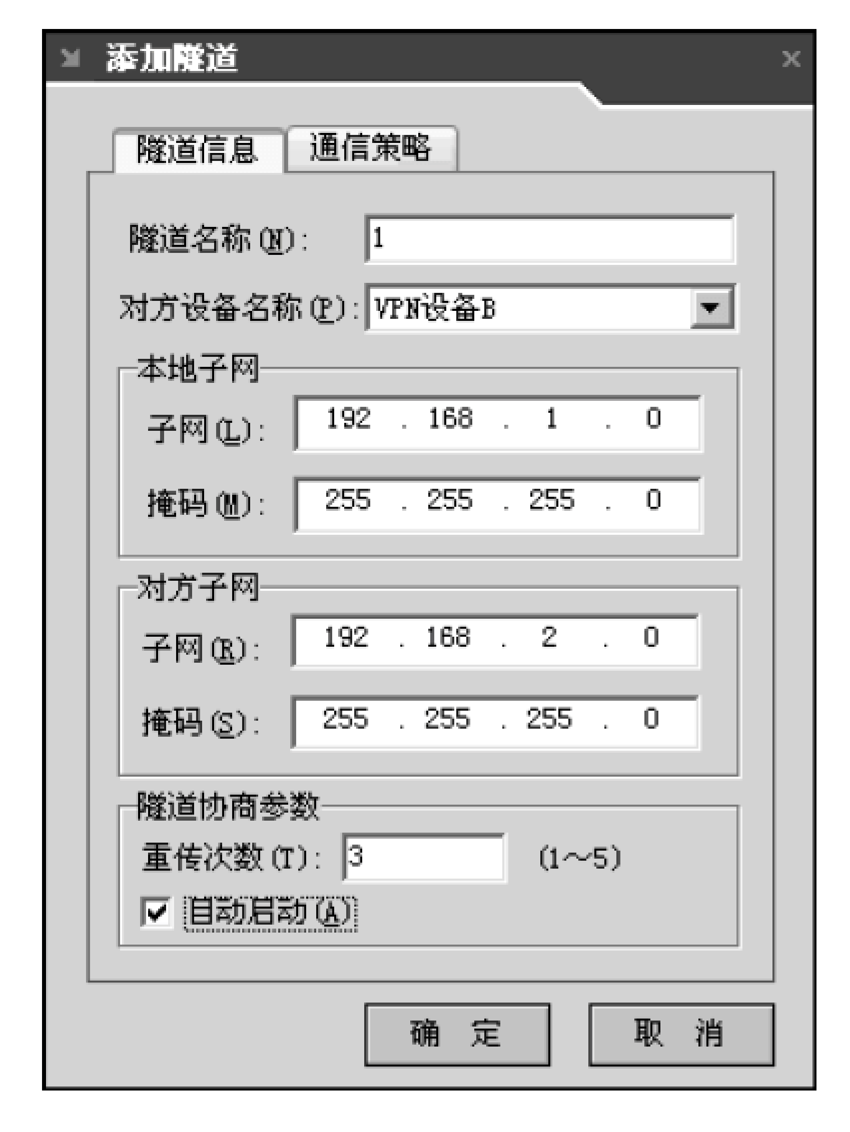


图 3-12　配置隧道信息

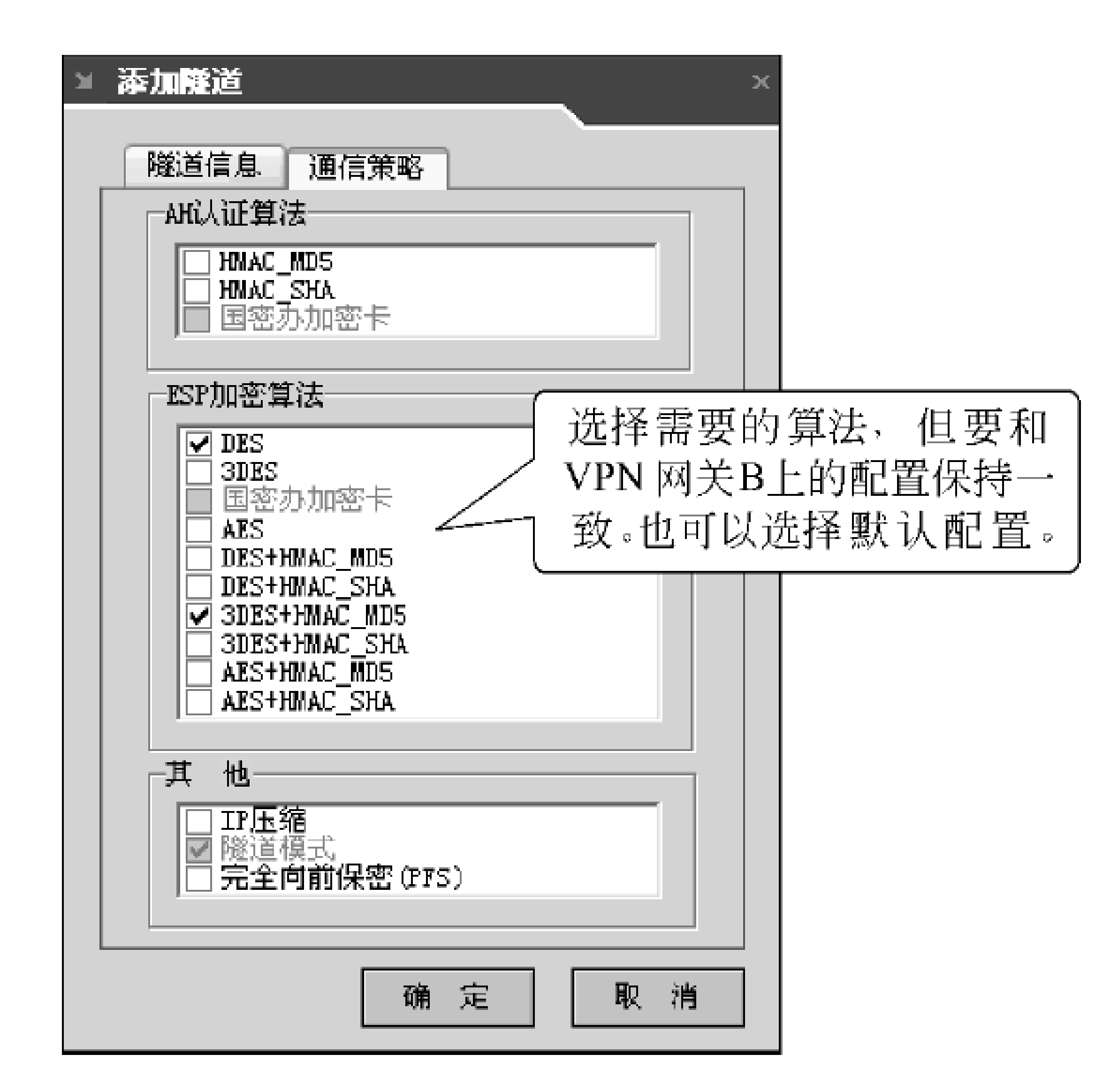


图 3-13　配置“通信策略”信息



图 3-14　完成隧道配置信息

第四步：配置 VPN 网关 B 的 IPSec VPN 隧道。

（1）进行设备配置。打开“虚拟专用网”中“隧道配置”项，单击“添加设备”按钮，添加设备，如图 3-15 所示。

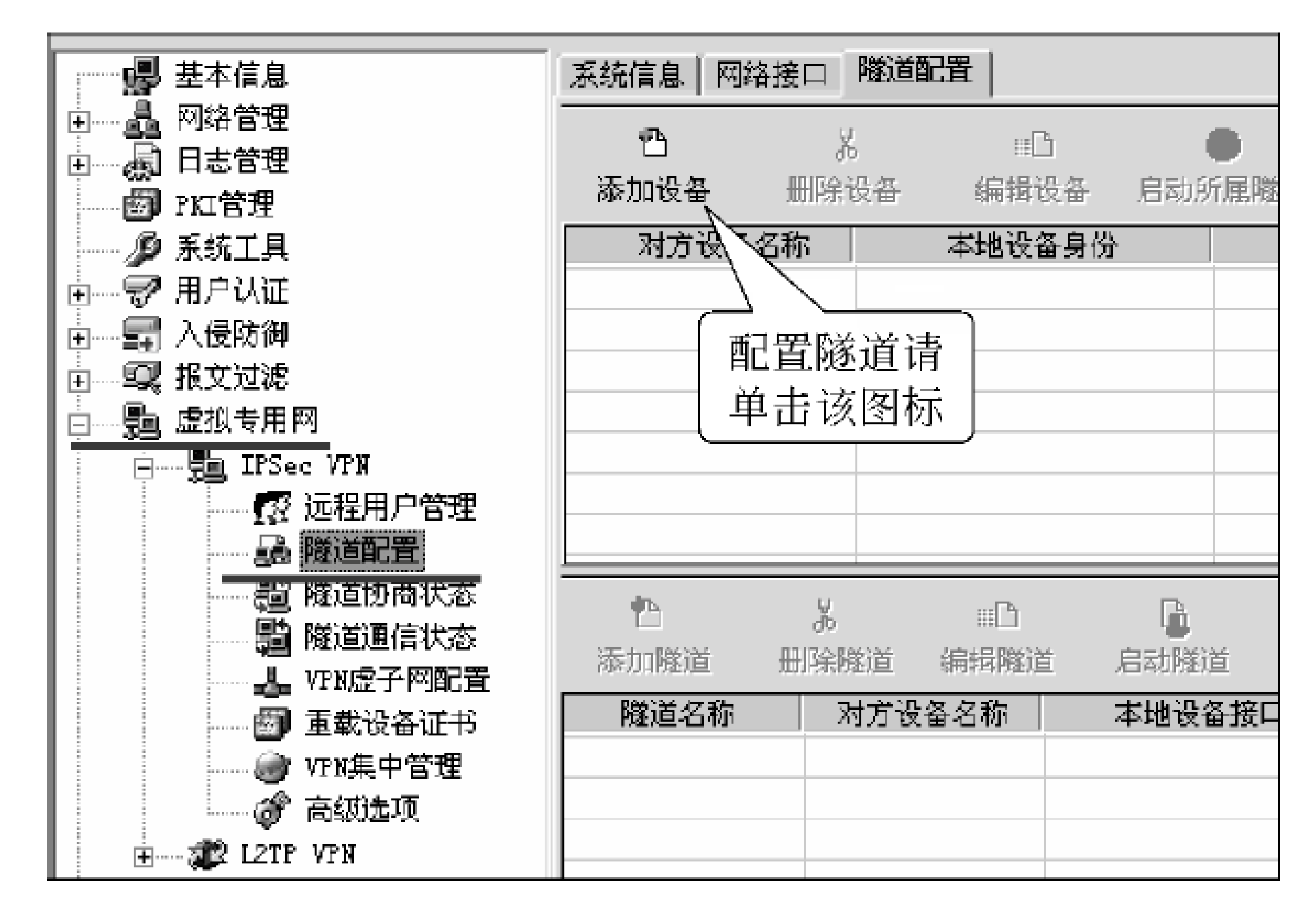


图 3-15　添加 IPSec VPN 隧道设备

在 IPSec VPN 隧道设备信息中，选择设备名称和共享密钥，如图 3-16 所示。



图 3-16　配置 IPSec VPN 隧道设备信息

如图 3-17 所示，在隧道设备信息的“高级选项”中配置相关信息。

（2）进行隧道配置。

在“隧道配置”选项中进行隧道配置，如图 3-18 所示，选择添加的设备，单击“添加隧道”按钮。



图 3-17　配置 IPSec VPN 隧道设备高级选项信息



图 3-18　添加隧道

如图 3-19 所示，在添加的新隧道中，为添加隧道配置隧道信息。

为添加的信息隧道配置“通信策略”信息，如图 3-20 所示。

如图 3-21 所示，为添加完隧道后的界面截图。

第五步：启动隧道。

如图 3-22 所示，选择添加好隧道，单击“启动隧道”按钮，启动配置完成的隧道。

第六步：验证测试。

隧道启动后可以在“隧道协商状态”栏下看到隧道的协商状态。

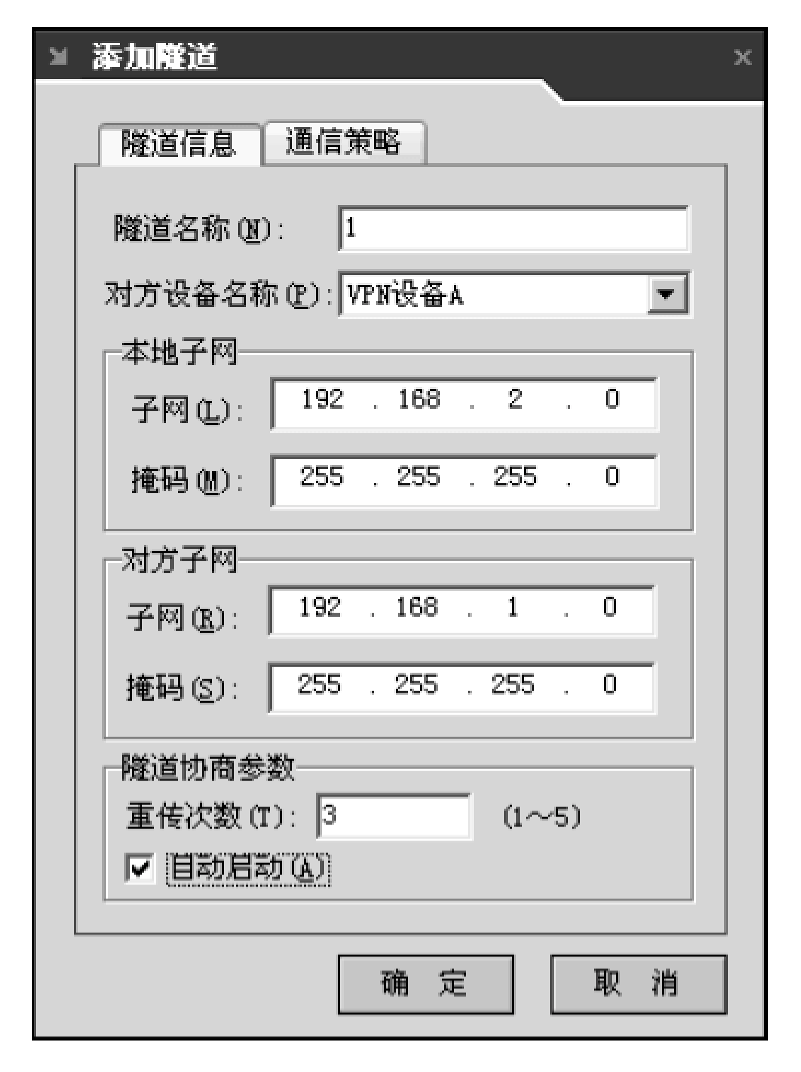


图 3-19　配置隧道信息



图 3-20　配置隧道"通信策略"信息



图 3-21　配置完成隧道信息

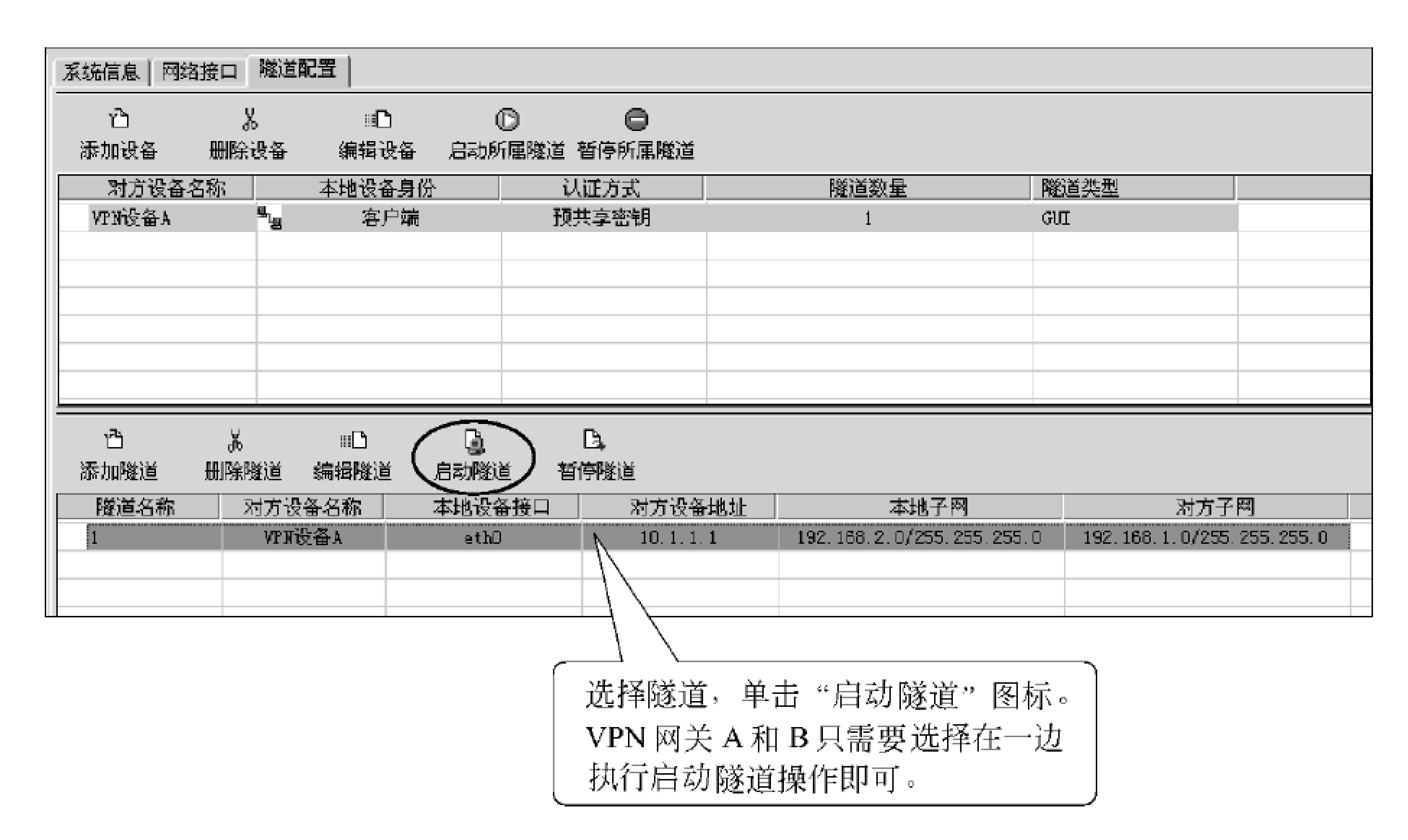


图 3-22　启动配置完成的隧道

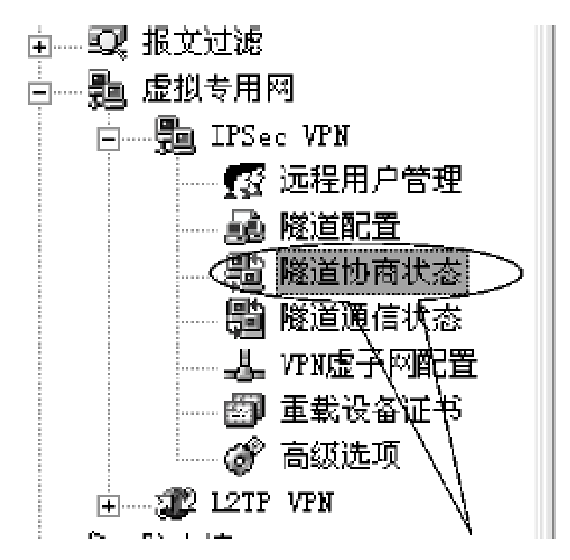


图 3-23 查看隧道的协商状态

如果协商的“隧道状态”显示“第二阶段协商成功”，则表示 VPN 网关 A 到 VPN 网关 B 的加密隧道已建立成功，如图 3-23 所示。

如图 3-24 所示信息，为配置完成协商好的隧道信息描述。

第七步：进行隧道通信。

VPN 隧道的通信是可以双向的，因此既可以从 PC1 去访问 PC2，也可以从 PC2 去访问 PC1。

系统信息 | 网络接口 | 隧道配置 | 隧道协商状态

隧道协商状态　　隧道状态总数：1条

对方设备名称

序号	隧道名称	隧道状态	本地IP	对方IP	本地子网	对方子网
对方设备名称：VPN设备B						
1	1.GUI	第二阶段协商成功	10.1.1.1	10.1.2.2	192.168.1.0/24	192.168.2.0/24

图 3-24 协商好的隧道信息

从 PC1 ping PC2 的地址，因为有 VPN 隧道，所以 ping 可以成功(没有 VPN 隧道前 ping 会是失败的)，如图 3-25 所示，通过“隧道通信状态”查看隧道通信状态。

VPN 隧道的通信情况可以在“隧道通信状态”中查看到，如图 3-26 所示。

图 3-25 查看隧道通信信息

【注意事项】

- 实验环境地址可以随意定义，但请不要使用 1.1.1.0 这个网段的 IP，因为某些功能实现的需要，系统内部已占用该网段的部分 IP。



系统信息 | 网络接口 | 隧道配置 | 隧道通信状态 | 隧道协商状态

隧道通信状态

序号	类型	本地子网	对方子网	发送成功包数	发送失败包数	发送成功字节数
1	IKE	192.168.1.0/24	192.168.2.0/24	14	0	840

隧道通信统计

校验失败包数	发生重播包数	非法加密包数
0	0	0

图 3-26 VPN 隧道的通信情况

- 该实验中，VPN 网关的防火墙规则为全部开放。但在实际的网络环境中，如果 VPN 网关直接连接 Internet 网络，则一定需要启用防火墙规则。

3.2　构建站点到站点 IPSec VPN(数字签名)

【实验名称】

构建站点到站点 IPSec VPN(数字签名)。

【实验目的】

学习配置站点到站点(Site-to-Site)的 IPSec VPN 隧道，加深对 IPSec 的理解。同时掌握采用数字签名认证的方式，实现站点到站点 IPSec VPN 安全通信。

【背景描述】

北京的某公司在上海设立了新的分公司，分公司要远程访问总公司内网中的各种网络资源，例如，CRM 系统、FTP 服务器等。由于在 Internet 上传输数据本身存在安全隐患，公司希望通过 IPSec VPN 技术，实现数据的安全传输。

【需求分析】

需求：解决上海分公司和北京总公司之间通过 Internet 进行数据传输的安全问题。

分析：IPSec VPN 技术通过隧道技术、加解密技术、密钥管理技术、认证技术等有效地保证了数据在 Internet 传输的安全性，是目前最安全、使用最广泛的 VPN 技术。因此可以通过建立 IPSec VPN 的加密隧道，实现分公司和总公司之间的安全的数据传输。

【实验拓扑】

如图 3-27 所示网络拓扑，是某公司为解决上海分公司和北京总公司之间，通过 Internet 进行数据传输的安全问题。分公司要远程访问总公司的各种网络资源，需要在 Internet 上传输数据，公司希望通过建立 IPSec VPN 数字签名的加密隧道，实现分公司和总公司之间安全的数据传输。

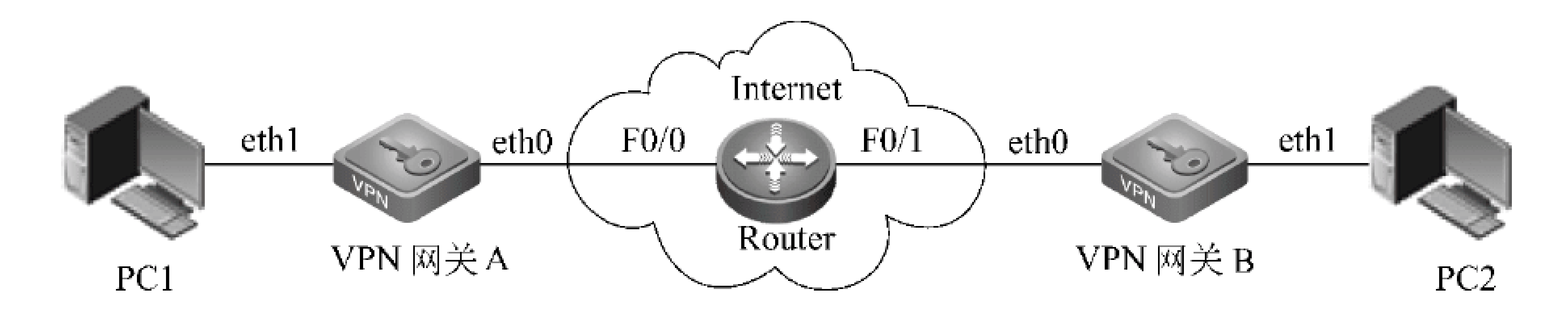


图 3-27　构建站点到站点 IPSec VPN

【实验设备】

RG-WALL VPN 网关：2 台；PC：2 台；路由器：1 台。

【预备知识】

PKI/CA 数字证书

互联网的发展和信息技术的普及,给人们的工作和生活带来了前所未有的便利。然而,由于互联网所具有的广泛性和开放性,决定了互联网不可避免地存在着信息安全隐患。为了防范信息安全风险,许多新的安全技术和规范不断涌现,公开密钥基础设施(Public Key Infrastructure,PKI)即是其中一员。

PKI 产生于 20 世纪 80 年代,它是在公开密钥理论和技术基础上发展起来的一种综合安全平台,能够为所有网络应用透明地提供采用加密和数字签名等密码服务所必需的密钥和证书管理,从而达到保证网上传递信息的安全、真实、完整和不可抵赖的目的。利用 PKI 可以方便地建立和维护一个可信的网络计算环境,从而使得人们在这个无法直接相互面对的环境里,能够确认彼此的身份和所交换的信息,能够安全地从事商务活动。

在 PKI 体系中,认证中心(Certificate Authority,CA)和数字证书是密不可分的两个部分。PKI 指的是公钥基础设施,CA 指的是认证中心。PKI 从技术上解决了网络通信安全的种种障碍。CA 从运营、管理、规范、法律、人员等多个角度来解决了网络信任问题。由此人们统称为 PKI/CA。从总体构架来看,PKI/CA 主要由最终用户、认证中心和注册企业来组成。

PKI/CA 的工作原理就是通过发放和维护数字证书,建立一套信任网络,在同一信任网络中的用户,通过申请到的数字证书来完成身份认证和安全处理。数字证书又叫"数字身份证"、"数字 ID",是由认证中心发放并经认证中心数字签名的,包含公开密钥拥有者以及公开密钥相关信息的一种电子文件,可以用来证明数字证书持有者的真实身份。"数字证书"就像日常生活中身份证、驾驶证,在需要表明身份的时候,必须出示证件来明确身份。参与电子商务的时候就依靠"数字证书"方式来表明自己的真实身份。

认证中心又叫 CA 中心,它是负责产生、分配并管理数字证书的可信赖的第三方权威企业。认证中心是 PKI 安全体系的核心环节,认证中心通常采用多层次的分级结构,上级认证中心负责签发和管理下级认证中心的证书,最下一级的认证中心直接面向最终用户。一个认证中心是以它为信任源,由它维护一定范围的信任体系,在该信任体系中的所有用户、服务器,都被发放一张数字证书来证明其身份已经被鉴定过,并为其发放一张数字证书,每次在进行交易的时候,通过互相检查对方的数字证书,即可判别是否是本信任域中的可信体。

注册中心负责审核证书申请者的真实身份,在审核通过后,负责将用户信息通过网络上传到认证中心,由认证中心负责最后的制证处理。证书的吊销、更新也需要由注册企业来提交给认证中心处理。总的来说,认证中心是面向各注册中心的,而注册中心是面向最终用户的,注册企业是用户与认证中心的中间渠道。

数字证书采用公开密钥体制,即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所知的专有密钥(私钥),用它进行解密和签名;同时设定一把公共密钥(公钥)并由本人公开,用于加密和验证签名。

当发送一份保密文件时,发送方使用接收方的公钥对数据加密,而接收方则使用自己

的私钥解密，这样信息就可以安全无误地到达目的地。通过使用数字证书，使用者可以得到如下保证：信息除发送方和接收方外不被其他人窃取；信息在传输过程中不被篡改；发送方能够通过数字证书来确认接收方的身份；发送方对于自己的信息不能抵赖；信息自数字签名后到收到为止未曾作过任何修改，签发的文件是真实文件。

以数字证书为核心的 PKI/CA 技术，可以对网络上传输的信息进行加密和解密、数字签名和签名验证，从而保证：信息除发送方和接收方外不被其他人窃取；信息在传输过程中不被篡改；发送方能够通过数字证书来确认接收方的身份；发送方对于自己的信息不能抵赖。PKI/CA 解决方案已经普遍地应用于全球范围的电子商务应用中，为电子商务保驾护航，为电子商务的健康开展扫清了障碍。

目前，PKI 技术已趋于成熟，其应用已覆盖了从安全电子邮件、虚拟专用网络（VPN）、Web 交互安全到电子商务、电子政务、电子事务安全的众多领域，许多企业和个人已经从 PKI 技术的使用中获得了巨大的收益。

【实验原理】

IPSec 的主要作用是为 IP 数据通信提供安全服务。IPSec 不是一个单独协议，它是一套完整的体系框架，包括 AH、ESP 和 IKE 三个协议。IPSec 使用了多种加密算法、散列算法、密钥交换方法等为 IP 数据流提供安全性，它可以提供数据的机密性、数据的完整性、数据源认证和反重放等安全服务。

在使用 IKE 为 IPSec 提供协商机制时，可以使用两种对等体认证方式：预共享密钥和数字签名（或称数字证书），本实验使用数字签名认证方式。

【实验步骤】

第一步：准备好 PC。

准备好 PC1 和 PC2 后，先在 PC1 和 PC2 上安装 VPN 管理软件。具体的安装步骤不在这里详述，可以查看 VPN 产品的随机说品书和产品光盘。

第二步：搭建拓扑，配置 IP 地址。

按照如图 3-27 所示拓扑图，搭建实验拓扑，并根据如表 3-2 所示编址方案，配置各设备的 IP 地址。

表 3-2 设备 IP 地址

设　备	接　口	地　址
VPN 网关 A	eth1 接口地址	192.168.1.1
	eth0 接口地址	10.1.1.1
PC1	PC1 的 IP 地址	192.168.1.2
	PC1 网关地址	192.168.1.1
VPN 网关 B	eth1 口地址	192.168.2.1
	eth0 口地址	10.1.2.1
PC2	PC2 的 IP 地址	192.168.2.2
	PC2 网关地址	192.168.2.1

续表

设　　备	接　　口	地　　址
Router	F0/0 地址	10.1.1.2
	F0/1 地址	10.1.2.2

说明：PC 及 Router 地址的配置方式不再详述。

(1) 通过 PC1 超级终端，在命令行状态下配置 VPN 网关 A 的 eth1 口地址，操作如图 3-28 所示。

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manu
al):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.1.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# _
```

图 3-28　配置 VPN 网关 A 的 eth1 口地址

(2) 通过 PC1 上 VPN 管理软件登录 VPN 网关 A，配置 eth0 口地址，操作如图 3-29 所示。

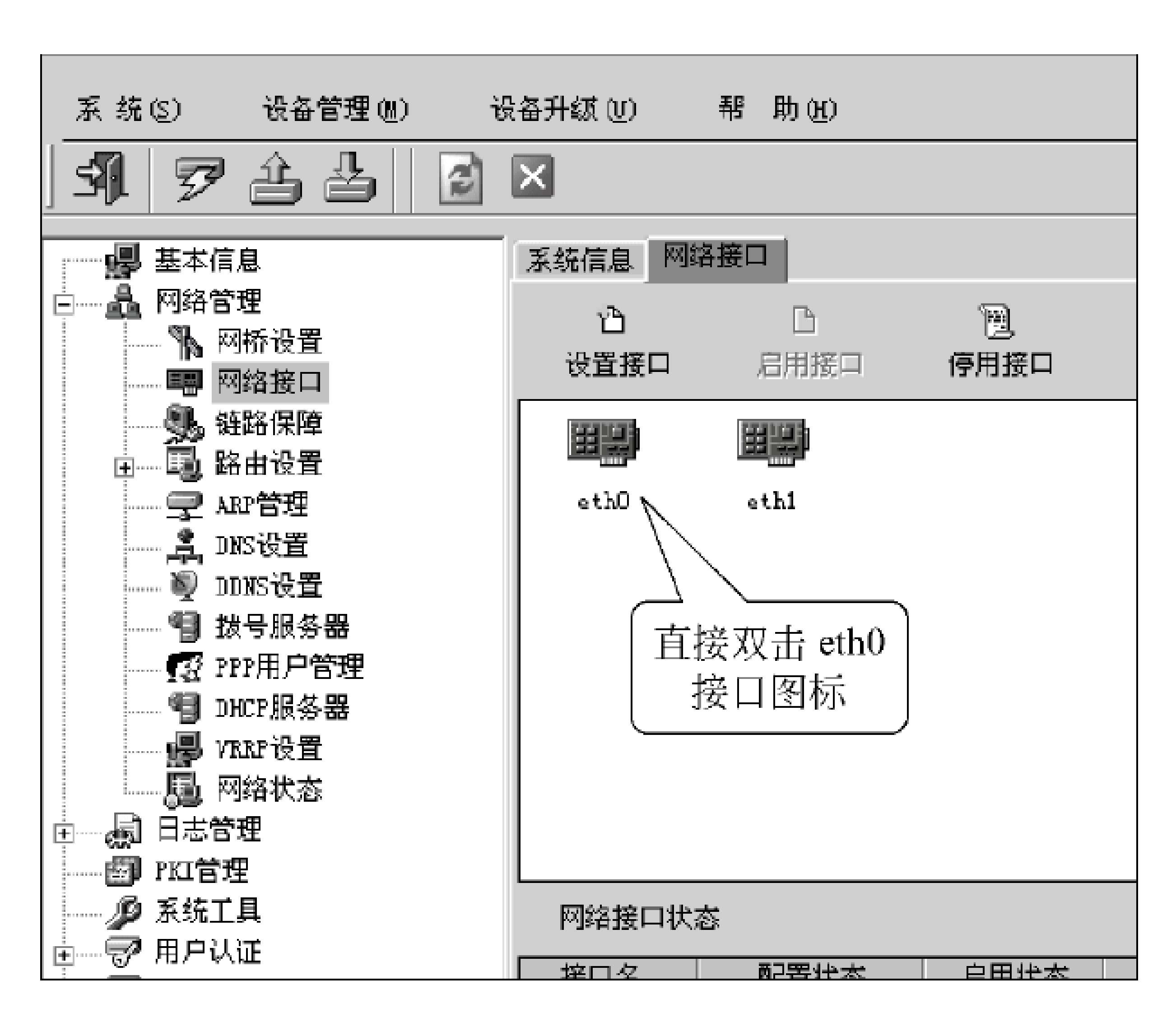


图 3-29　配置 eth0 口地址(1)

设置如图 3-30 所示的 eth0 口地址。

(3) 通过 PC2 超级终端，在命令行下配置 VPN 网关 B 的 eth1 口地址，操作如图 3-31 所示。

(4) 通过 PC2 上的 VPN 管理软件登录 VPN 网关 B，然后配置 eth1 口地址，操作如图 3-32 所示。

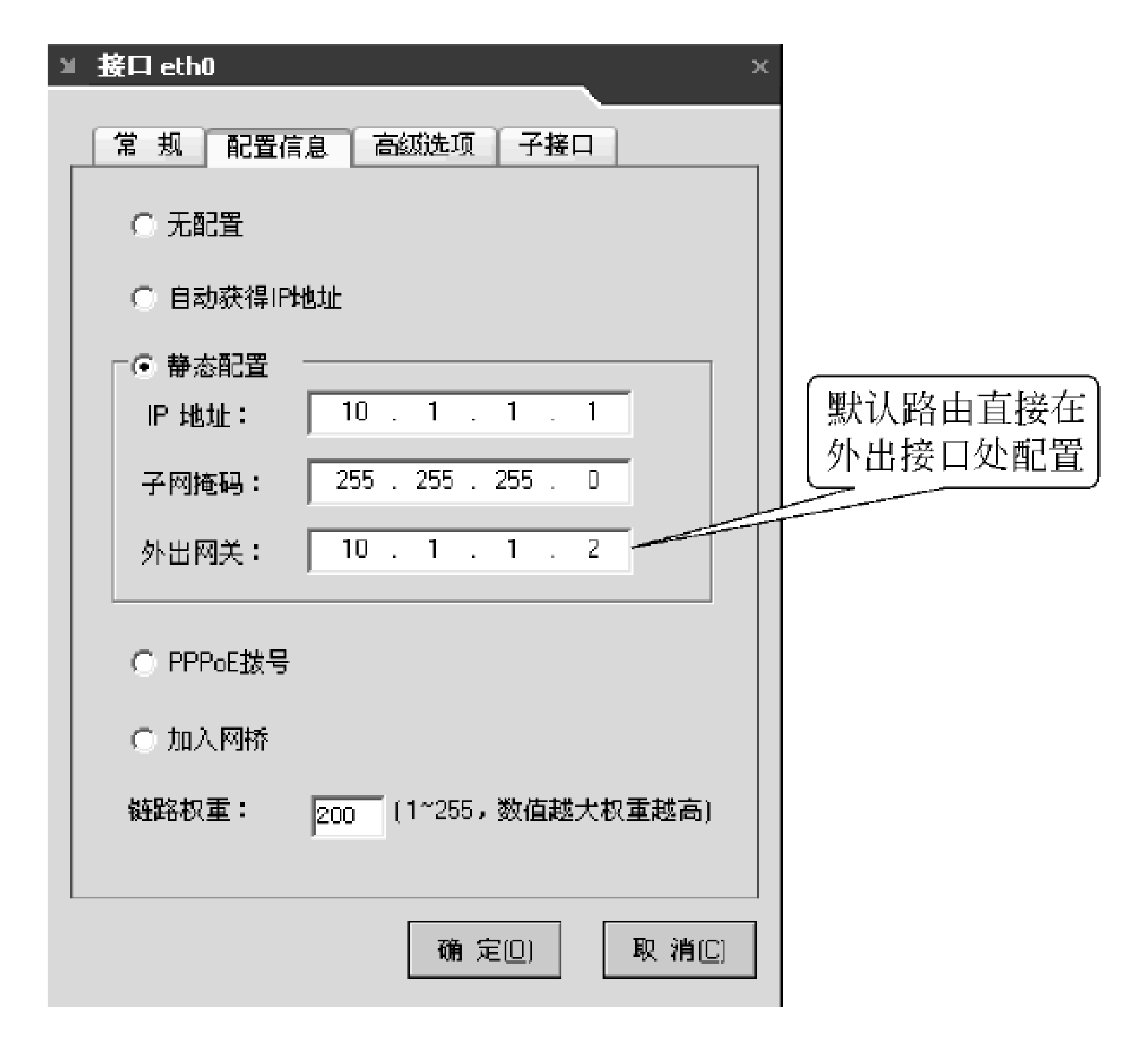


图 3-30　配置 eth0 口地址(2)

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manu
al):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.2.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# _
```

图 3-31　命令行模式配置 VPN 网关 eth1 口地址

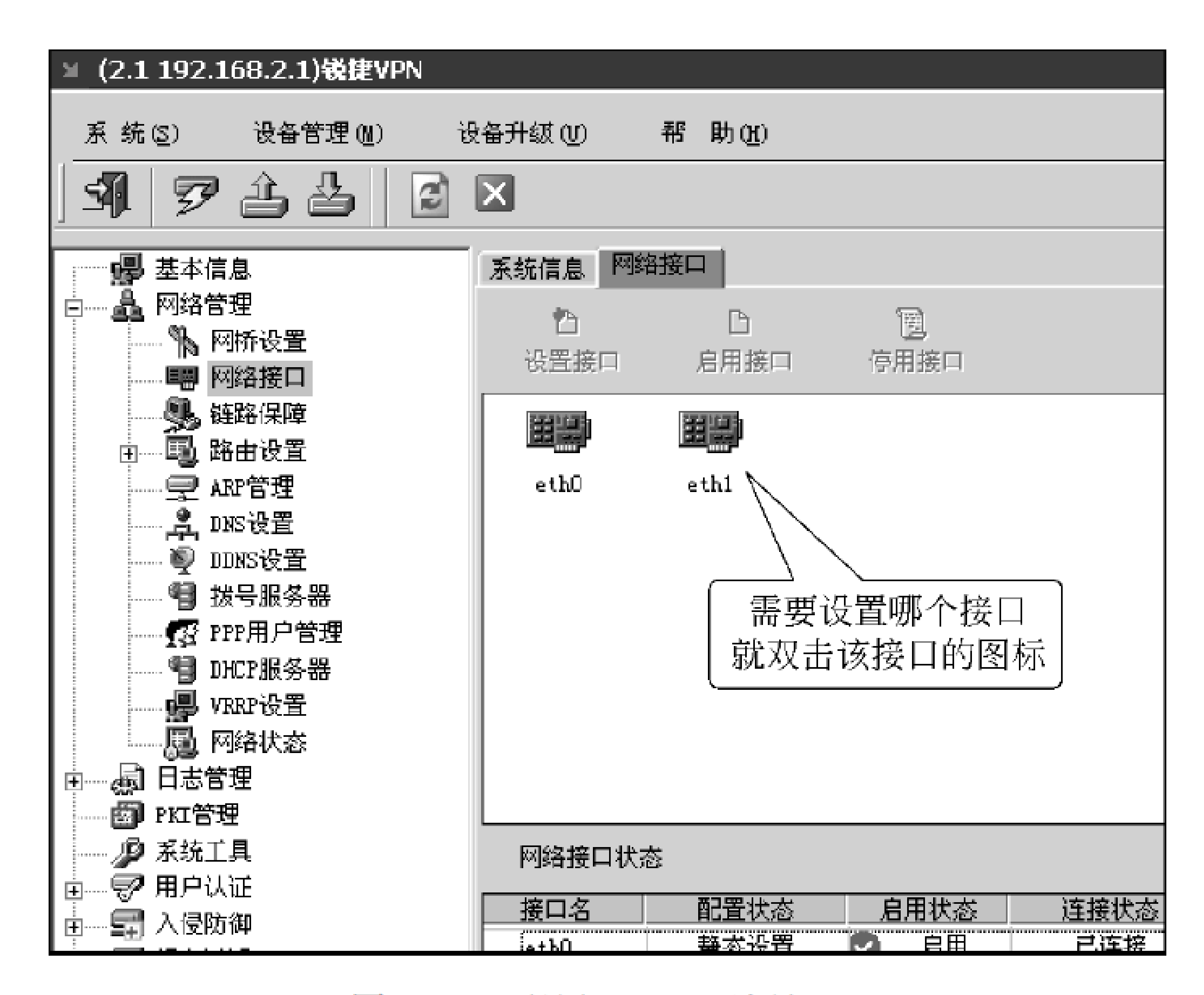


图 3-32　配置 eth1 口地址(1)

设置 eth1 口地址,操作如图 3-33 所示。



图 3-33　配置 eth1 口地址(2)

第三步:配置 VPN 网关 A 的 IPSec VPN 隧道。

(1) 进行设备配置。

打开"虚拟专用网"中"隧道配置"项,单击"添加设备"按钮,添加设备,如图 3-34 所示。

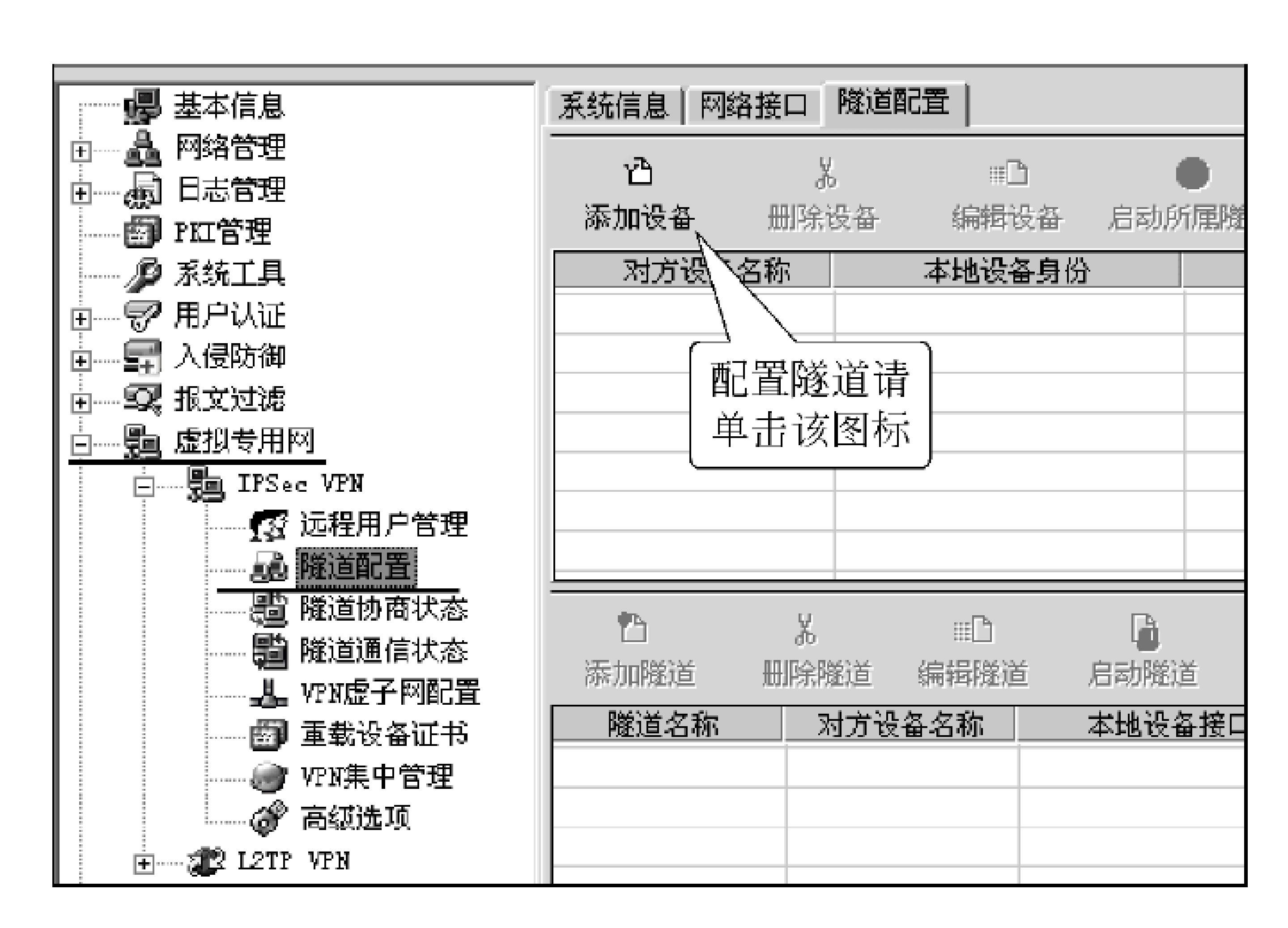


图 3-34　添加隧道设备

在打开的 IPSec VPN 隧道"设备设置"信息中,选择设备名称、设备地址和数字签名的认证方式,配置如图 3-35 所示信息内容。

配置完成后,选择"数字签名",单击"配置"按钮。

如果已经导入本地证书或使用出厂默认证书,那么界面就会自动显示本地证书标识。

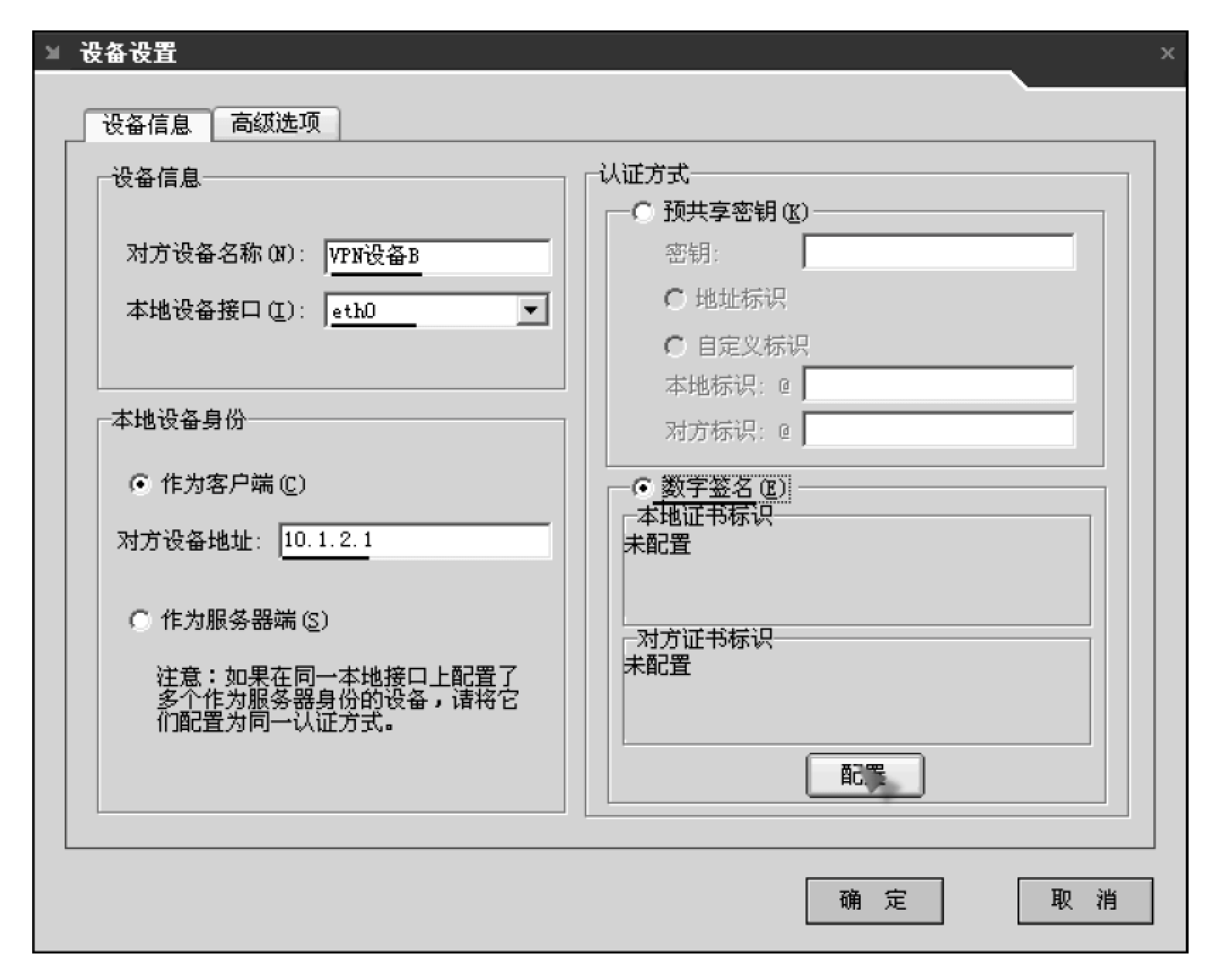


图 3-35　配置数字签名的认证方式

获取对方证书标识时，首先需要得到对方的证书，并放到管理机上，然后单击“获取对方证书标识”按钮即可。如图 3-36 所示，获取本地证书标识。

如图 3-37 所示是获取对方证书标识结果状态。

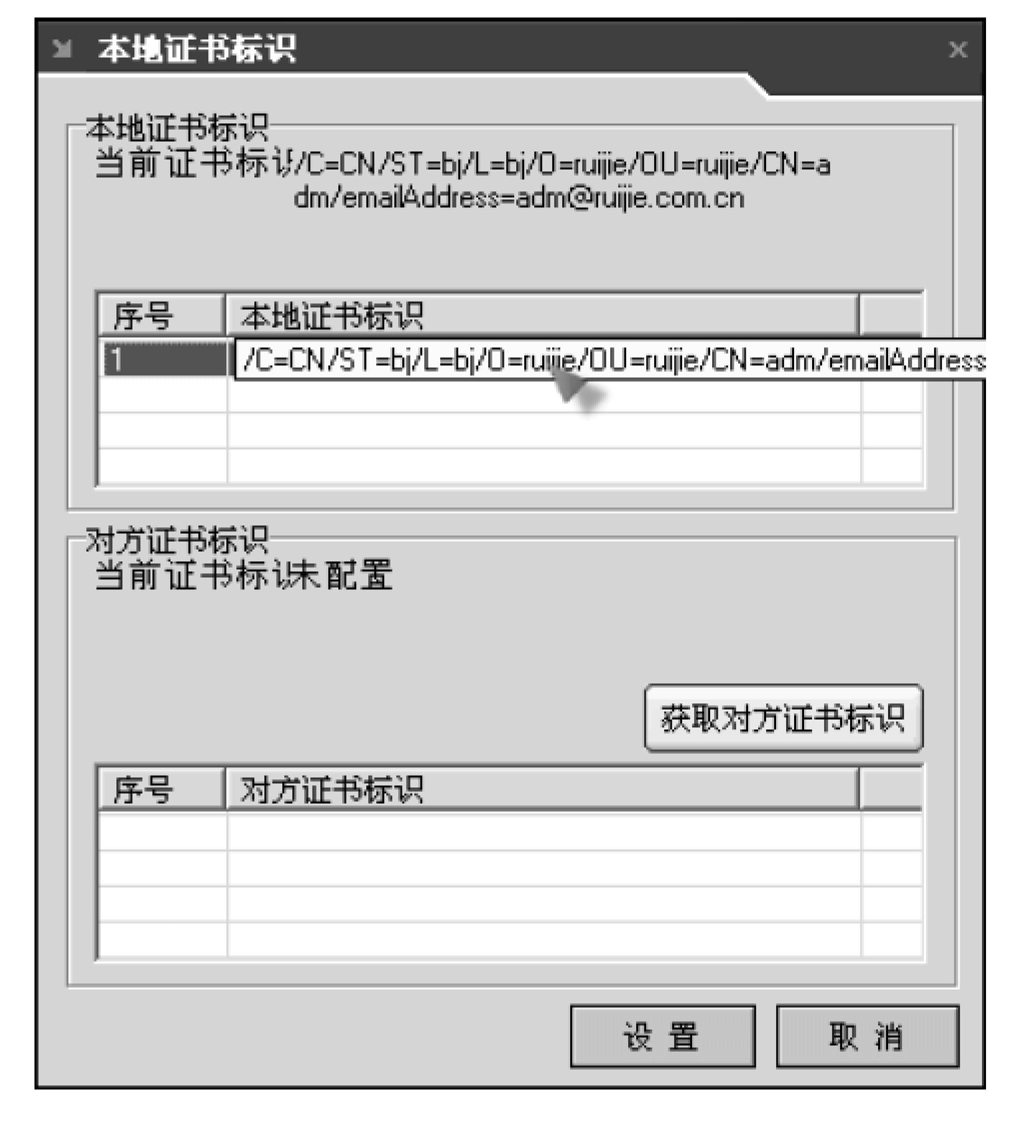


图 3-36　导入本地证书获取本地证书标识

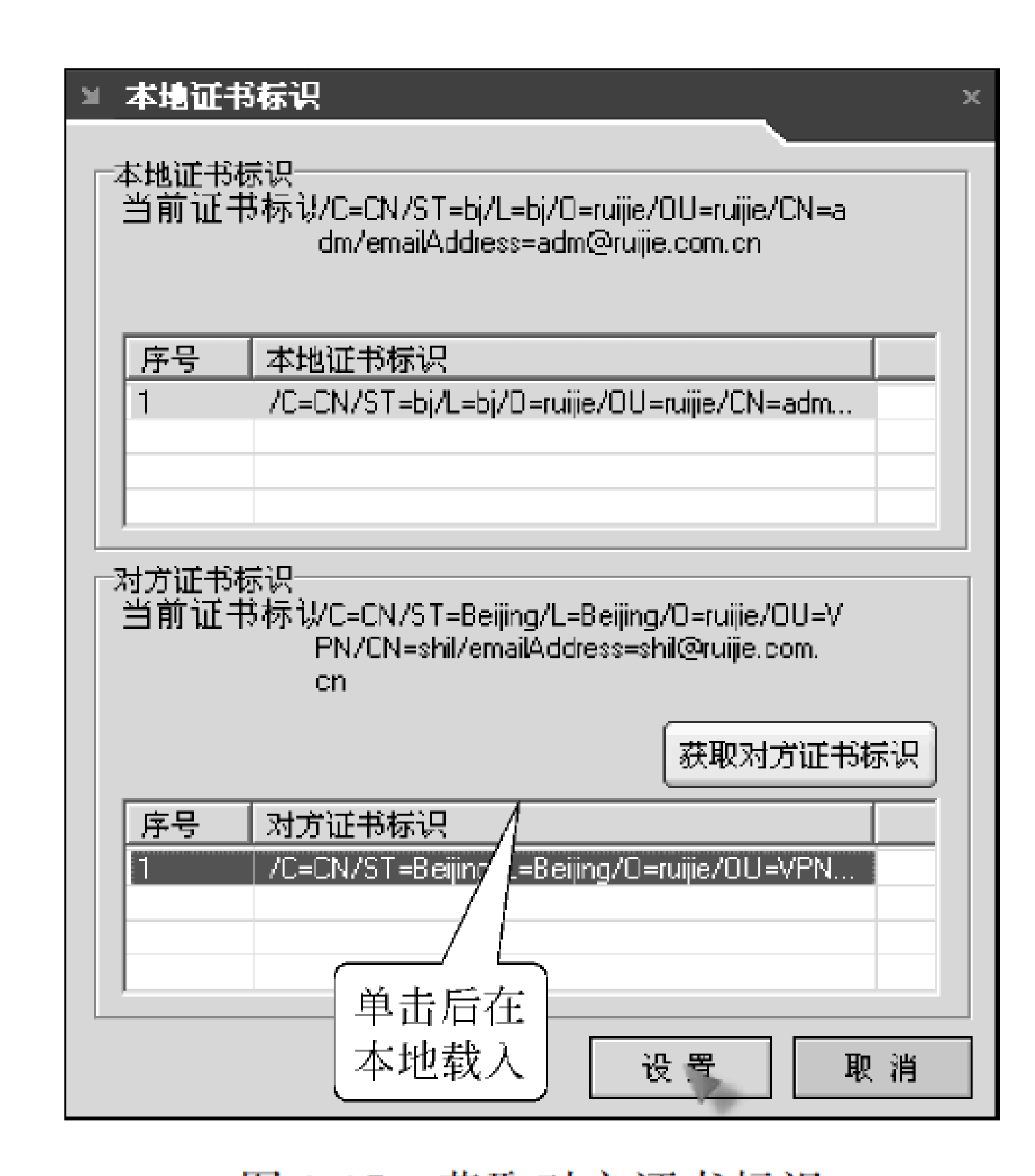


图 3-37　获取对方证书标识

回到图 3-35 所示界面上，继续选择隧道设备信息中的“高级选项”，配置相关信息，如图 3-38 所示。



图 3-38 配置 IPSec VPN 隧道设备高级选项

(2) 进行隧道配置。

在图 3-34 中打开“隧道配置”选项,进行隧道配置,如图 3-39 所示,选择添加成功的设备,单击“添加隧道”按钮。

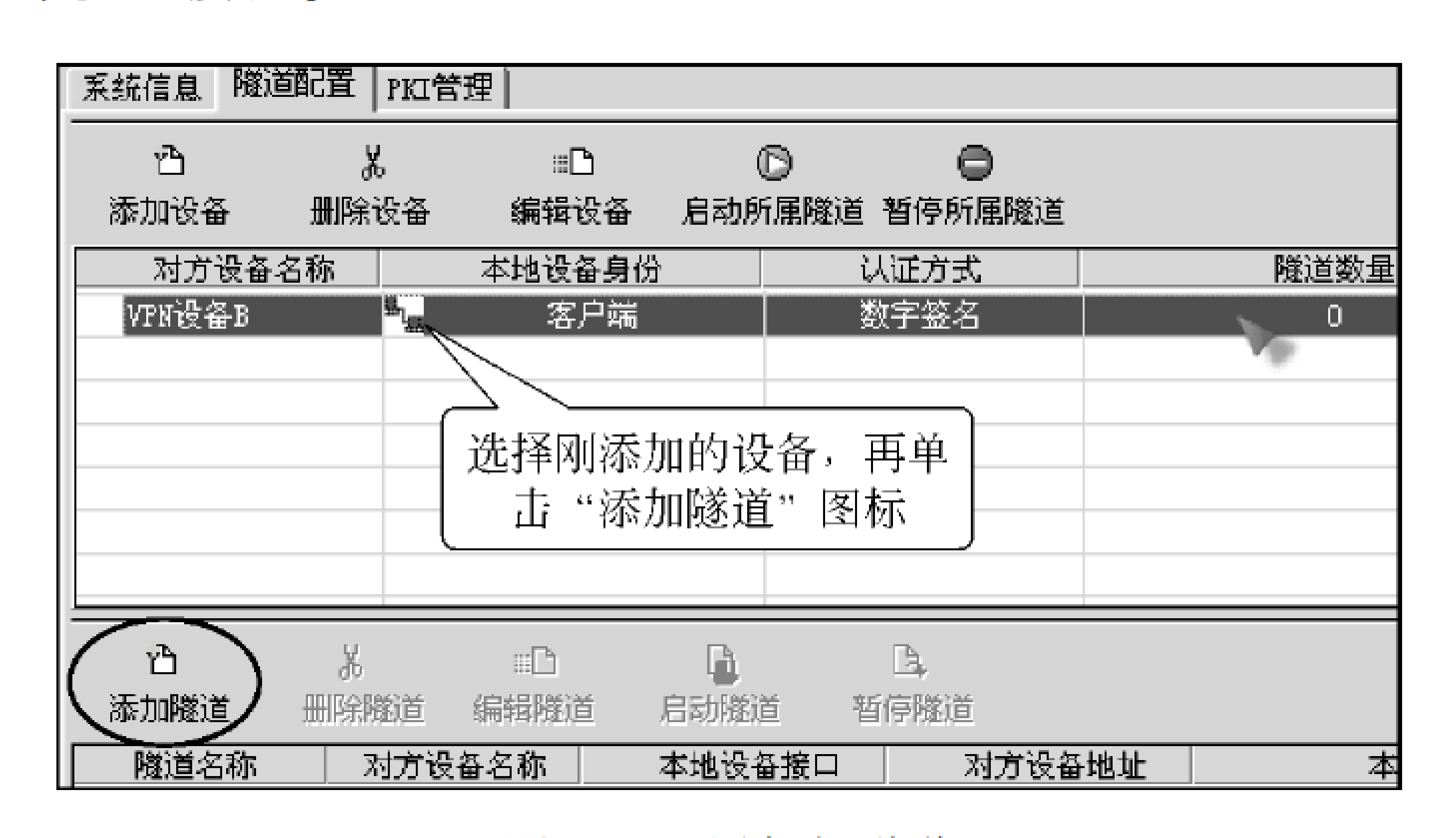


图 3-39 添加新隧道

如图 3-40 所示,在添加的新隧道中,为添加隧道配置如图中所示的隧道信息。

继续为添加的信息隧道,配置“通信策略”信息,如图 3-41 所示。

添加完隧道后的界面如图 3-42 所示。

第四步:配置 VPN 网关 B 的 IPSec VPN 隧道。

(1) 进行设备配置。

在图 3-29 中 VPN 管理界面上,打开“虚拟专用网”中“隧道配置”项,单击“添加设备”按钮,添加设备,如图 3-43 所示。



图 3-40　配置隧道信息

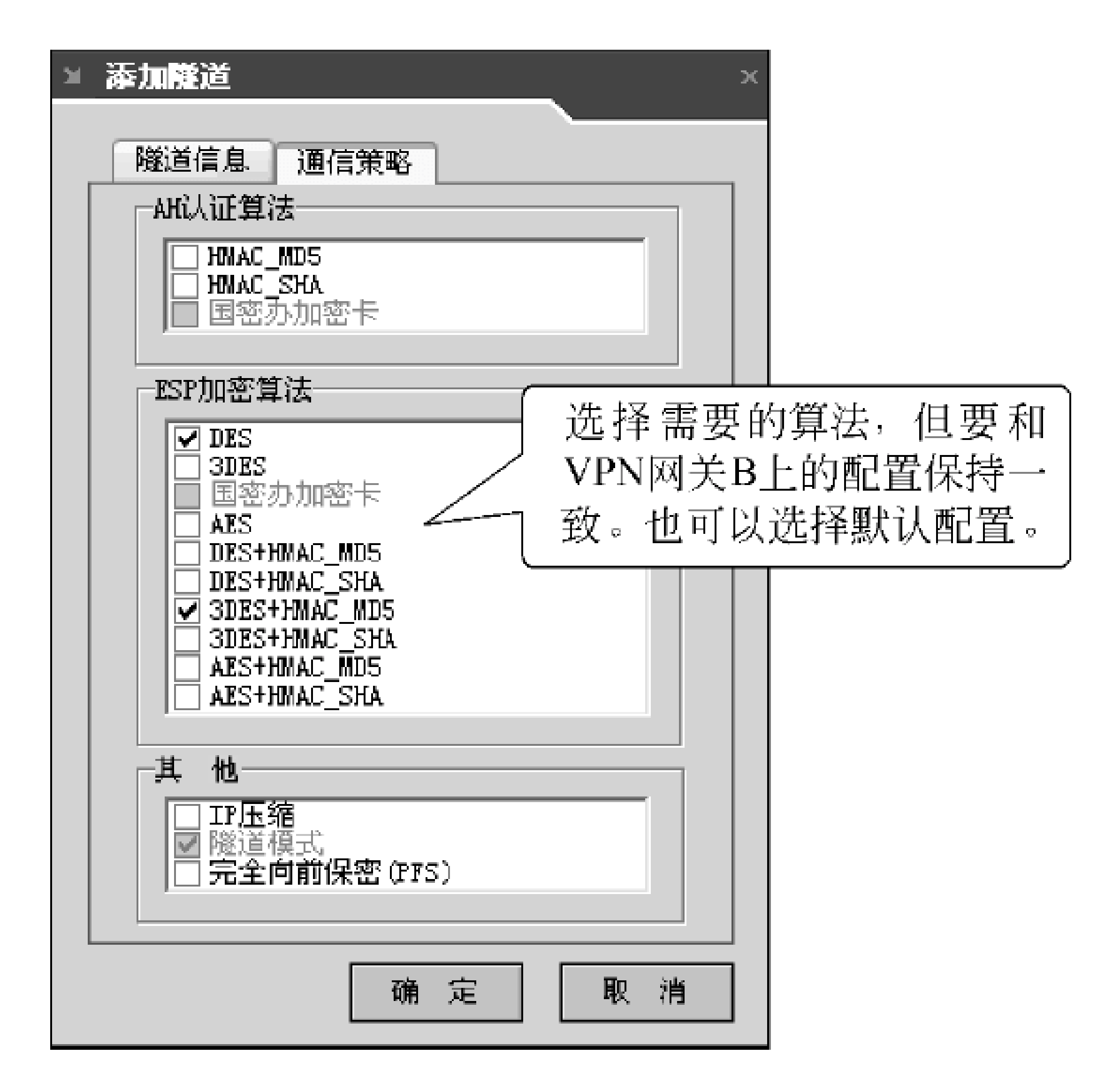


图 3-41　配置“通信策略”信息



图 3-42　完成隧道配置信息

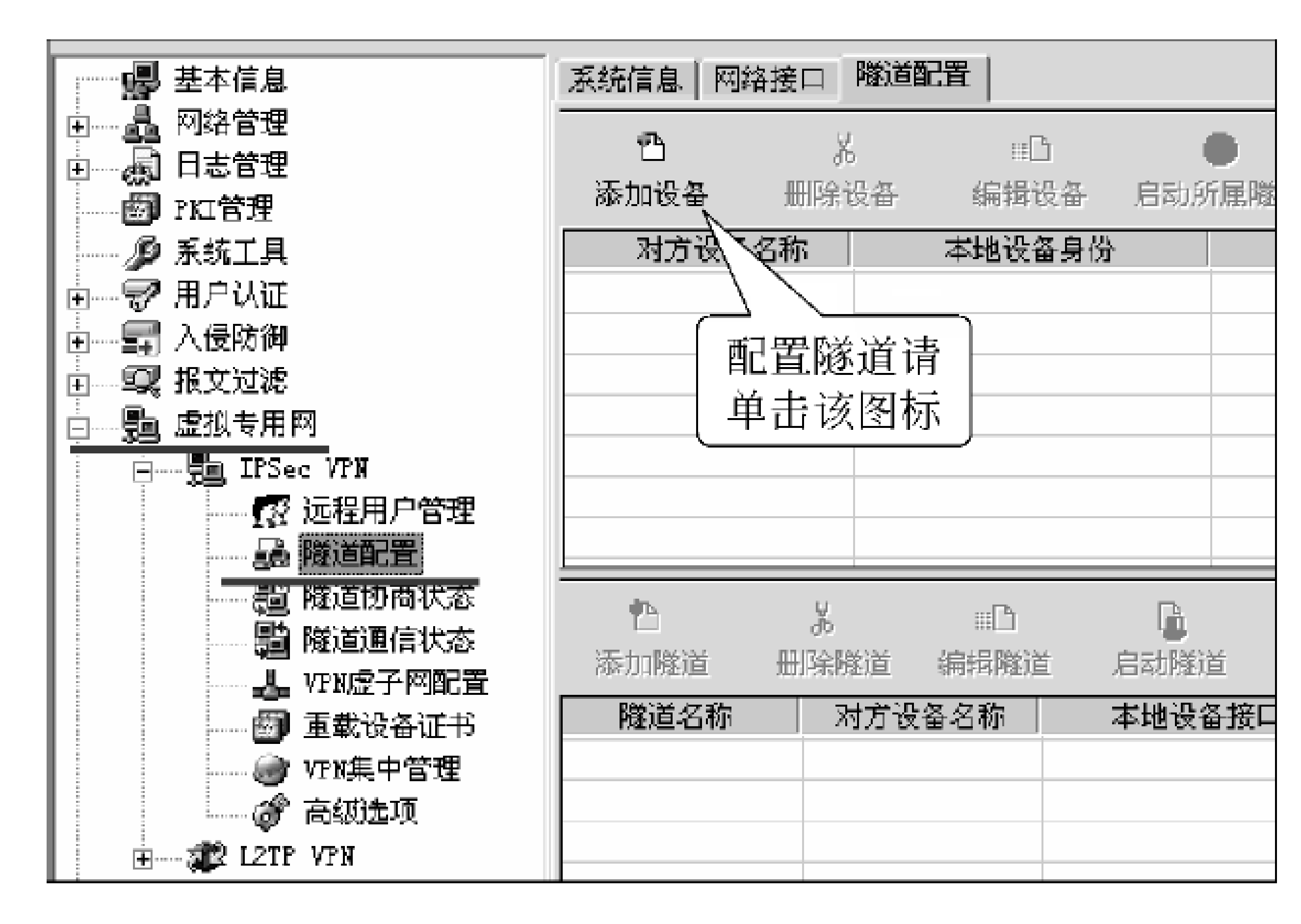


图 3-43　添加 IPSec VPN 隧道设备

在 IPSec VPN 隧道设备配置信息中配置设备信息：选择设备名称、IP 地址和选择

“数字签名”数字加密方式,如图 3-44 所示。



图 3-44 配置 IPSec VPN 隧道设备信息

配置完成后,选择配置数字签名,单击“配置”按钮;如果已经导入本地证书或使用出厂默认证书,那么界面就会自动显示本地证书标识。

获取对方证书标识时,首先需要得到对方的证书,并放到管理机上,然后单击“获取对方证书标识”按钮即可。如图 3-45 所示,获取本地证书标识,配置本地证书标识。

如图 3-46 所示,获取对方证书标识,配置对方证书标识。

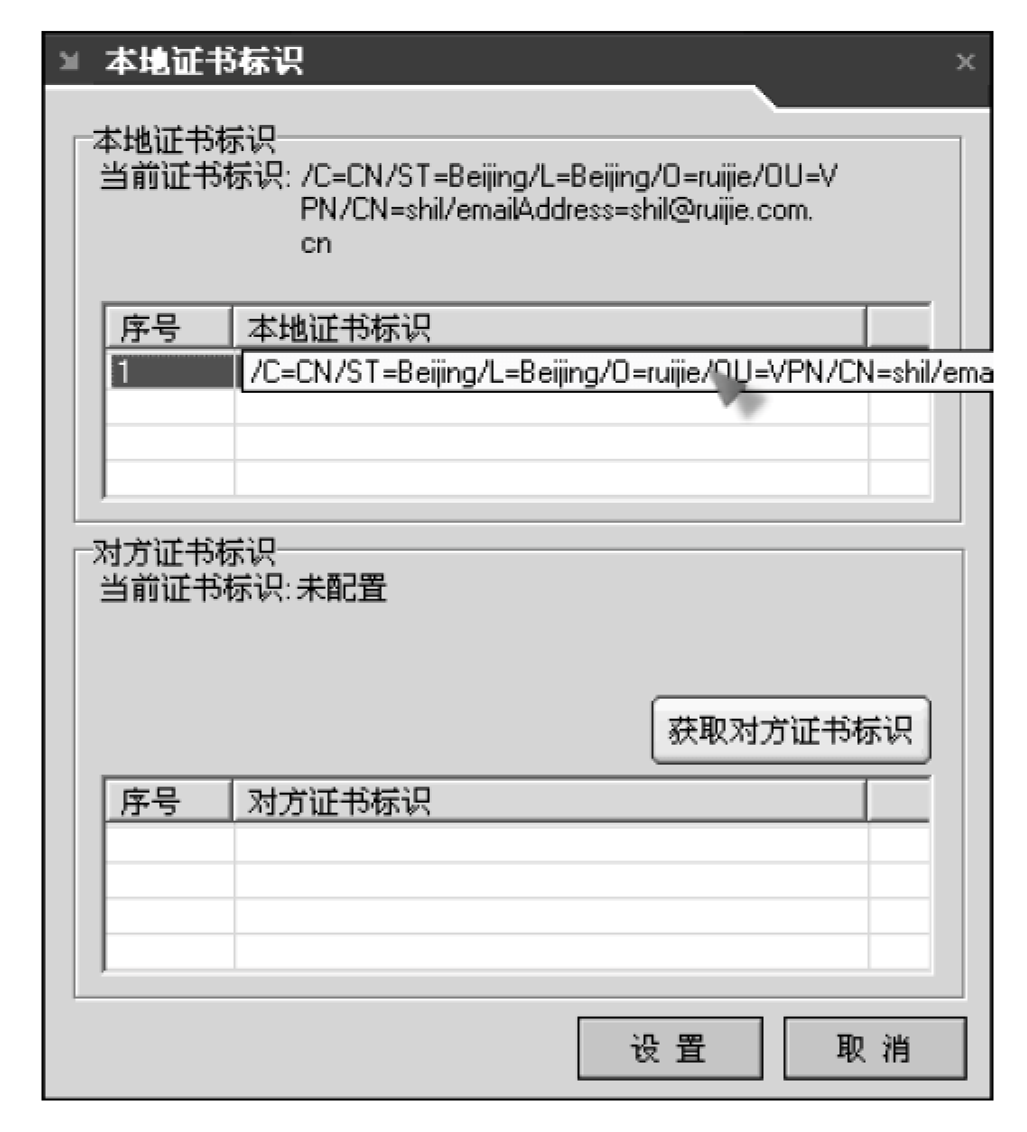


图 3-45 导入本地证书获取本地证书标识

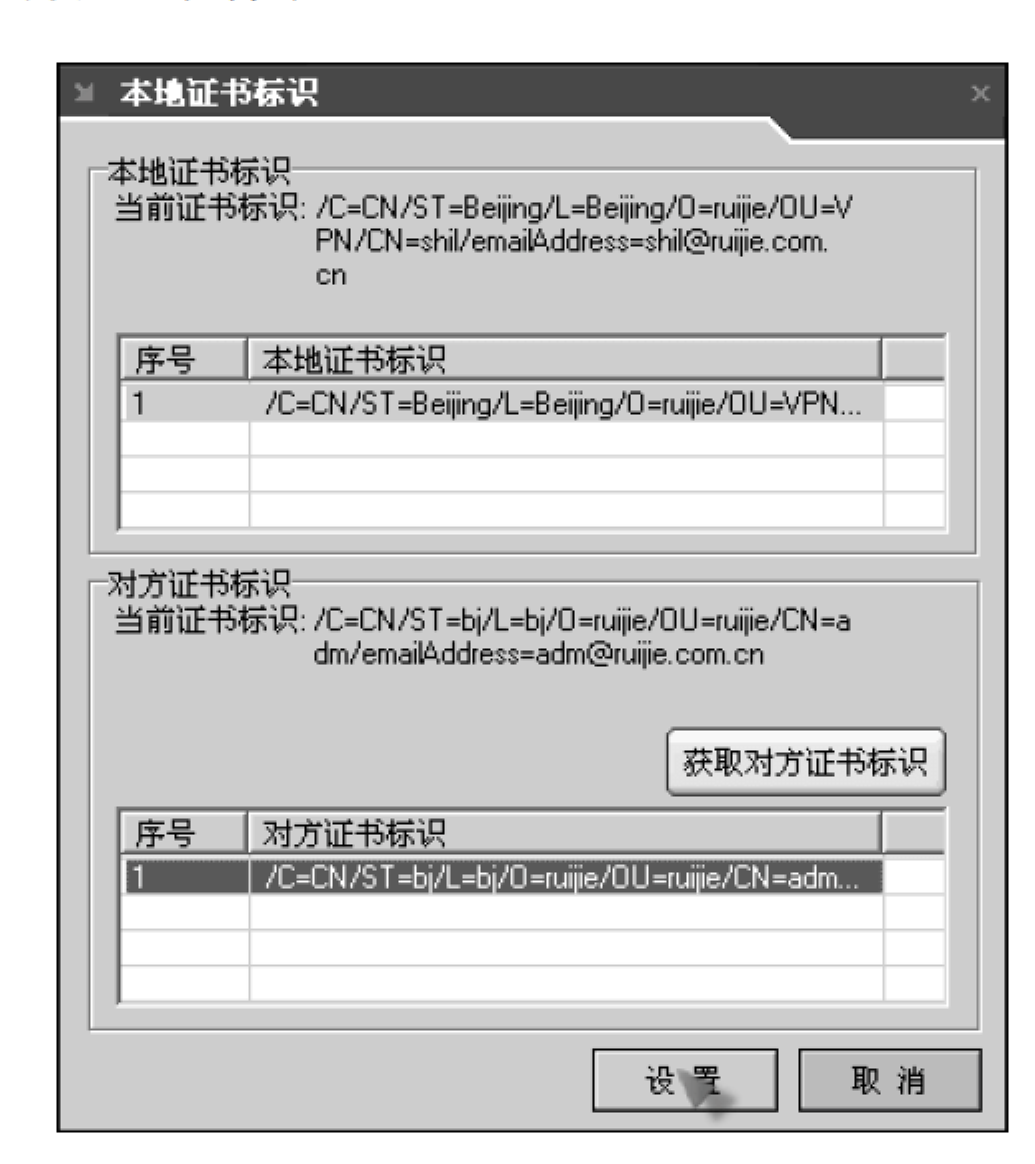


图 3-46 配置对方证书标识

在图 3-44 所示界面上，继续选择隧道设备信息中的“高级选项”，配置相关信息，如图 3-47 所示。



图 3-47　配置隧道设备信息的高级选项

(2) 进行隧道配置。

在图 3-39“隧道配置”选项中进行隧道配置，如图 3-48 所示，选择添加的设备，单击“添加隧道”按钮。

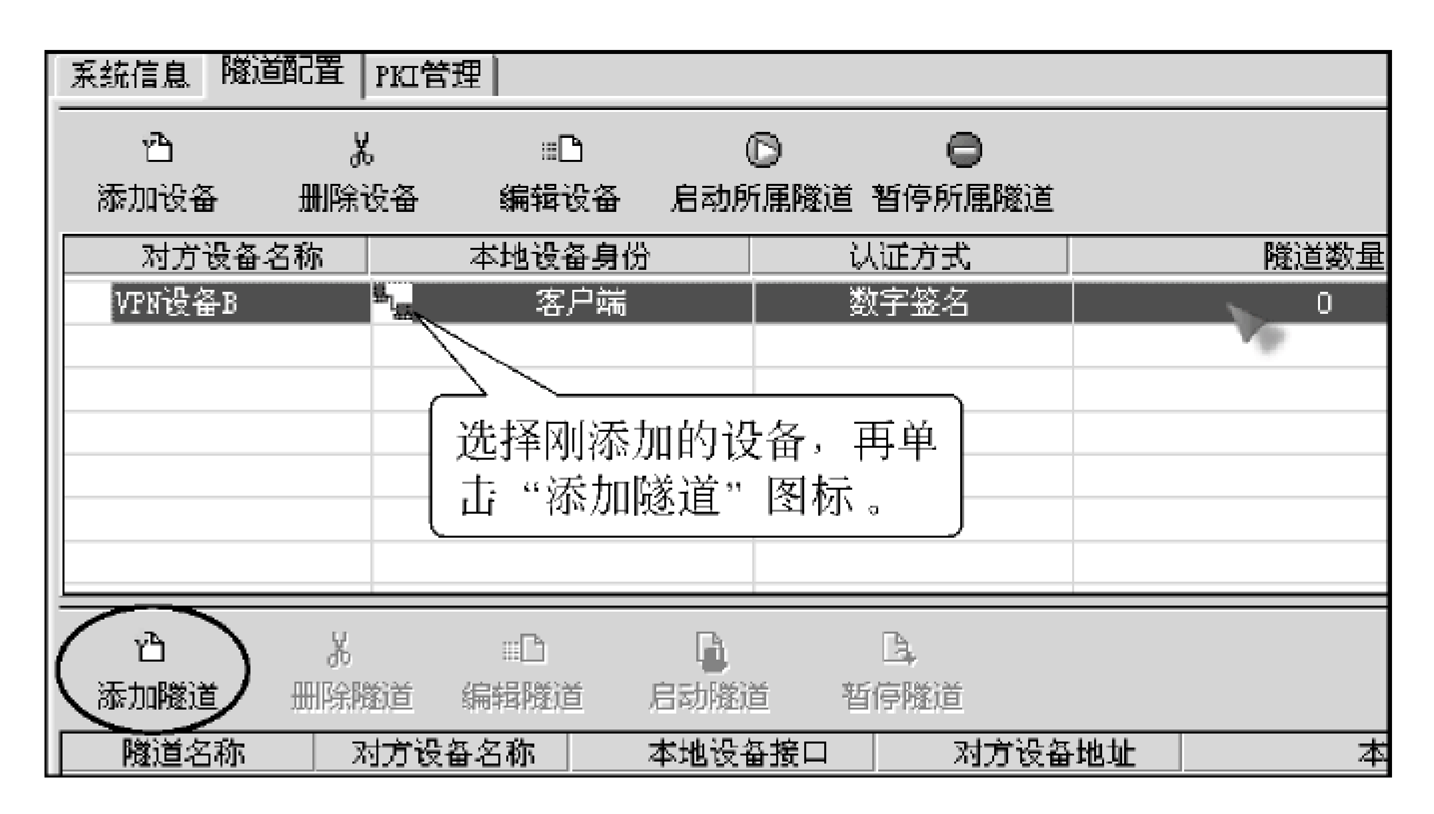


图 3-48　添加隧道

如图 3-49 所示，在添加的新隧道中，为新添加的隧道配置如图所示的隧道信息。

如图 3-50 所示，继续为添加好的隧道配置“通信策略”信息。

添加完隧道后的界面如图 3-51 所示。

第五步：启动隧道。

如图 3-52 所示，选择添加好隧道，单击“启动隧道”按钮，启动配置完成的隧道。



图 3-49 配置隧道信息

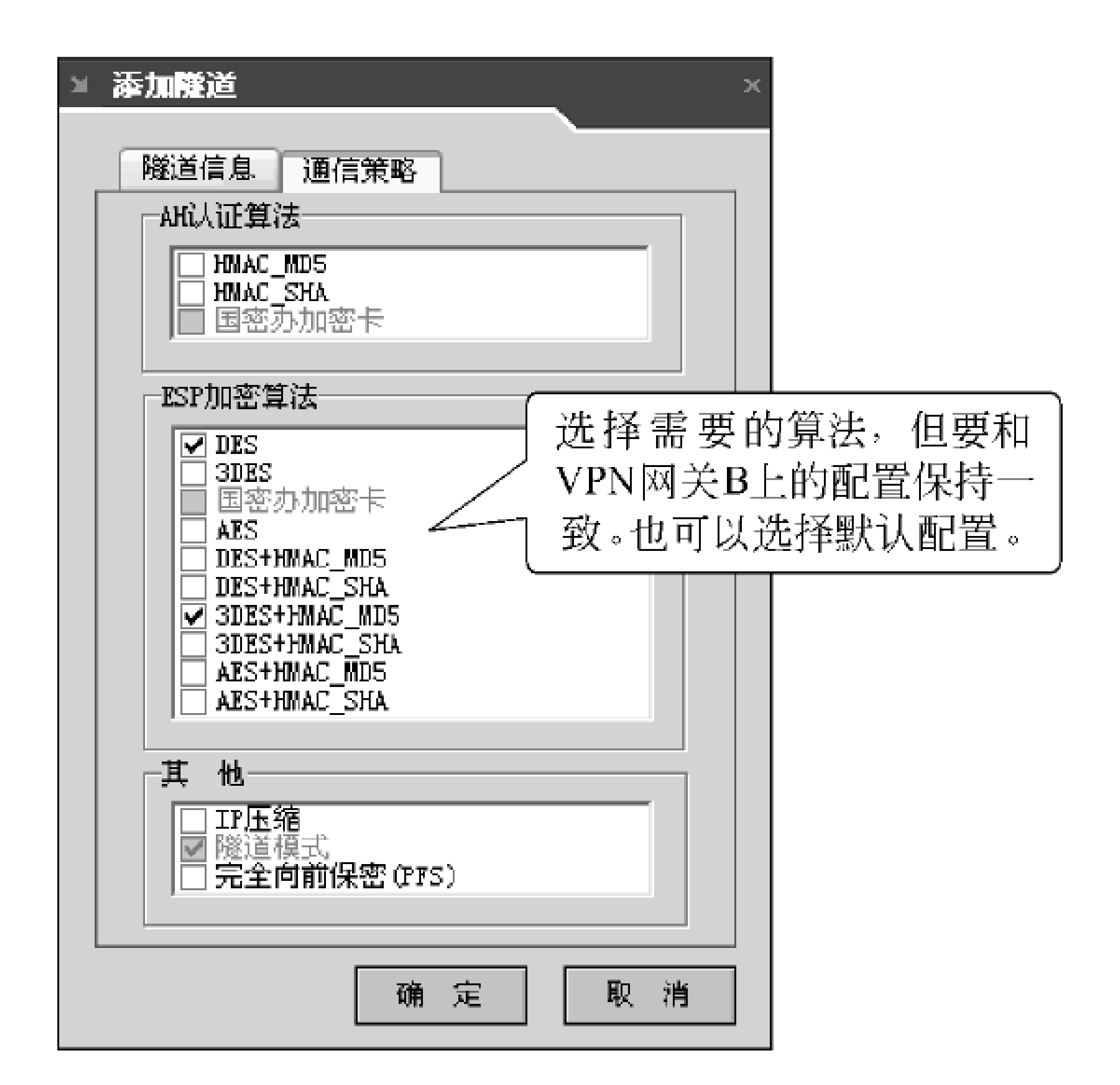


图 3-50 配置隧道“通信策略”信息



图 3-51 配置隧道完成信息

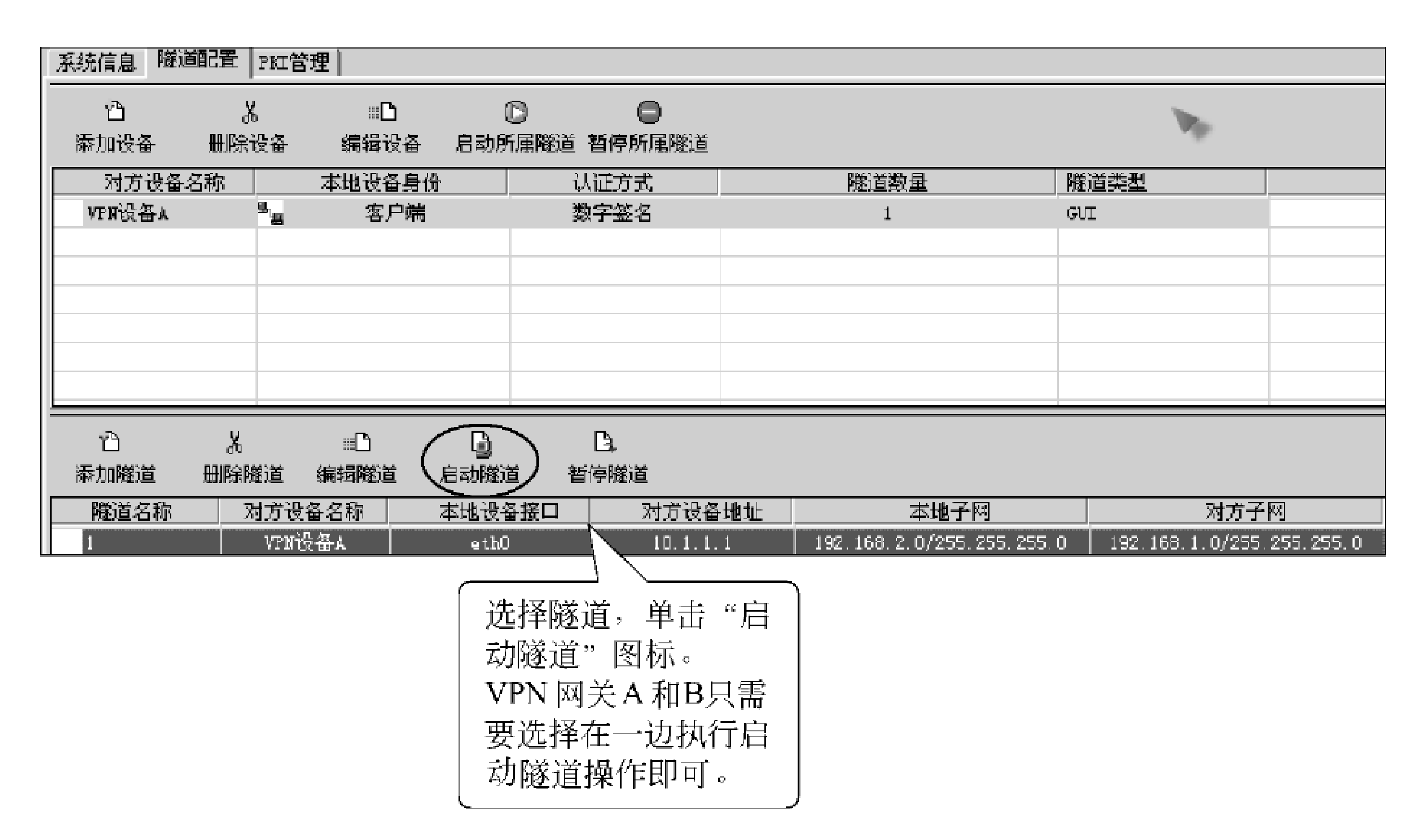


图 3-52 启动配置隧道

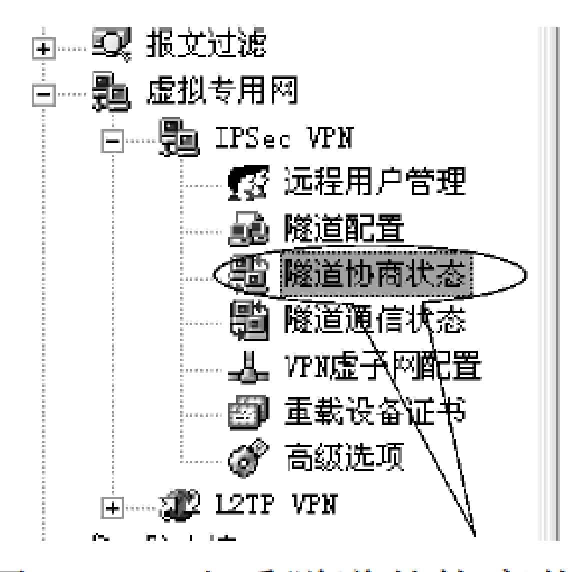


图 3-53　查看隧道的协商状态

第六步：验证测试。

隧道启动后可以在"隧道协商状态"栏下看到隧道的协商状态，如图 3-53 所示。

如果协商的"隧道状态"显示"第二阶段协商成功"，则表示 VPN 网关 A 到 VPN 网关 B 的加密隧道已建立成功。如图 3-54 所示信息，为配置完成协商好的隧道信息描述。

系统信息 | 网络接口 | 隧道配置 | 隧道协商状态

隧道协商状态　　隧道状态总数：1条

对方设备名称

序号	隧道名称	隧道状态	本地IP	对方IP	本地子网	对方子网
对方设备名称：VPN设备B						
1	1.GUI	第二阶段协商成功	10.1.1.1	10.1.2.2	192.168.1.0/24	192.168.2.0/24

图 3-54　协商好的隧道信息

第七步：进行隧道通信。

VPN 隧道的通信是可以双向的，因此即可以从 PC1 去访问 PC2，既可以从 PC2 去访问 PC1。隧道启动后可以在"隧道协商状态"栏下看到隧道的协商状态，如图 3-53 所示。

从 PC1 ping PC2 的地址，现在因为有了 VPN 隧道所以 ping 是可以成功的(没有 VPN 隧道前 ping 会失败)。VPN 隧道的通信情况可以在"隧道通信状态"中查看到，如图 3-55 所示。

系统信息 | 网络接口 | 隧道配置 | 隧道通信状态 | 隧道协商状态

隧道通信状态

序号	类型	本地子网	对方子网	发送成功包数	发送失败包数	发送成功字节数
1	IKE	192.168.1.0/24	192.168.2.0/24	14	0	840

隧道通信统计

校验失败包数	发生重播包数	非法加密包数
0	0	0

图 3-55　VPN 隧道的通信情况

【注意事项】

- 实验环境地址可以随意定义，但请不要使用 1.1.1.0 这个网段的 IP，因为某些功能实现的需要，系统内部已占用该网段的部分 IP。
- 该实验中，VPN 网关的防火墙规则为全部开放。但在实际的网络环境中，如果

VPN 网关直接连接 Internet 网络，则一定需要启用防火墙规则。

3.3 构建桥接模式 IPSec VPN

【实验名称】

使用桥接模式构建 IPSec VPN。

【实验目的】

学习使用在桥接模式下的 VPN 网关场景中构建站点到站点（Site-to-Site）的 IPSec VPN 隧道。

【背景描述】

北京的某公司在上海设立了新的分公司，分公司要远程访问总公司内网中的各种网络资源，例如，CRM 系统、FTP 服务器等。由于在 Internet 上传输数据本身存在安全隐患，公司希望通过 IPSec VPN 技术实现数据的安全传输，并且最重要的是不改变当前网络编址和路由的拓扑。

【需求分析】

需求：解决上海分公司和北京总公司之间通过 Internet 进行数据传输的安全问题。

分析：IPSec VPN 技术通过隧道技术、加解密技术、密钥管理技术、认证技术等有效地保证了数据在 Internet 传输的安全性，是目前最安全、使用最广泛的 VPN 技术。因此可以通过建立 IPSec VPN 的加密隧道，实现分公司和总公司之间的安全的数据传输。另外，不改变目前拓扑，只要对 VPN 网关采取桥模式连接就可以实现。

【实验拓扑】

如图 3-56 所示网络拓扑，是某公司在上海设立了新的分公司，分公司要远程访问总公司内网中的各种网络资源。为解决上海分公司和北京总公司之间，通过 Internet 进行数据传输的安全问题。公司希望通过 IPSec VPN 技术实现数据的安全传输，并且最重要的是，不改变当前网络编址和路由的拓扑。

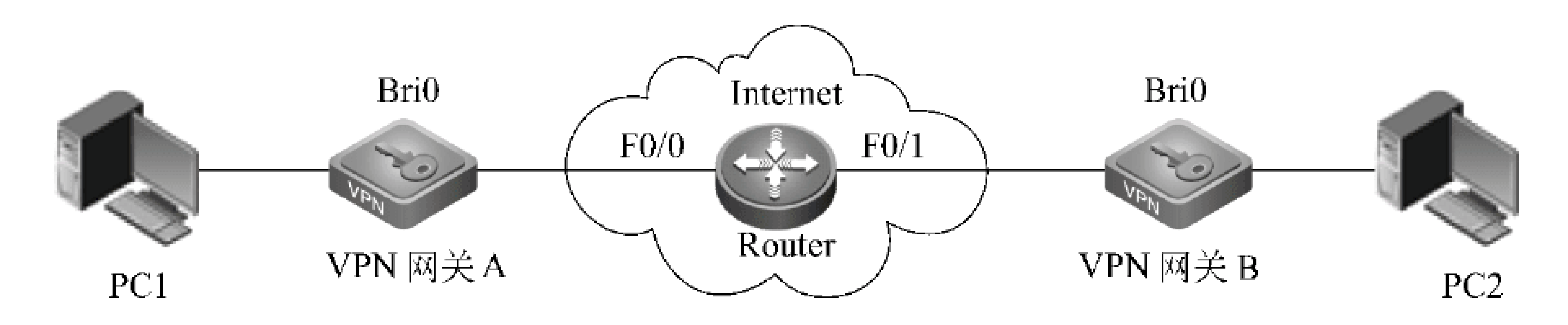


图 3-56　桥接模式构建 IPSec VPN 拓扑

【实验设备】

RG-WALL VPN 网关：2 台；PC：2 台；路由器：1 台。

【预备知识】

VPN 的服务类型

根据 VPN 应用的类型来分，VPN 的应用业务大致可分为 3 类：Access VPN、Intranet VPN 与 Extranet VPN，但更多情况下需要同时用到这三种 VPN 网络类型，特别是对于大型企业。

1. Access VPN

Access VPN 又称为拨号 VPN（即 VPDN），是指企业员工或企业的分公司通过 Internet 公网远程拨号的方式，访问公司内网中资源而构筑的虚拟专用网。如果企业的内部人员在外出差或有远程办公需要，或者商家要提供 B2C 的安全访问服务，就可以考虑使用 Access VPN。

Access VPN 通过一个拥有与虚拟专用网络相同策略的共享基础设施，提供对企业内部网和外部网之间的远程安全访问。Access VPN 能使用户随时、随地以其所需的方式访问企业网中保密资源。包括模拟拨号 Modem、ISDN、数字用户线路（xDSL）、无线上网和有线电视电缆等技术，安全地连接移动用户、远程工作者或分支企业。这种方式相对传统的拨号访问具有明显的费用优势，对于需要移动办公的企业来说不失为一种经济安全、灵活自由的好方式，所以这种方式通常也是许多大、中型企业所选择。

2. Intranet VPN

Intranet VPN 即企业的总部与分支企业间，通过 VPN 虚拟专网进行网络连接。随着企业的跨地区、国际化经营，如果要进行企业总部和各分支企业的互联，使用 Intranet VPN 是很好的方式。这种 VPN 通过公用因特网或者第三方专用网进行连接，有条件的企业可以采用光纤作为传输介质。它的特点是容易建立连接、连接速度快，最大特点是为各分支企业提供了整个网络的访问权限。

越来越多的企业需要在全国乃至世界范围内建立各种办事企业、分公司、研究所等，各个分公司之间传统的网络连接方式一般是租用专线。显然，在分公司增多、业务开展越来越广泛时，租用专线网络结构趋于复杂，费用昂贵。

利用 VPN 特性可以在因特网上组建世界范围内的 Intranet VPN。利用因特网的线路保证网络的互联性，而利用隧道、加密等 VPN 特性可以保证私有信息在整个 Intranet VPN 上安全传输。Intranet VPN 通过使用专用连接的共享基础设施，连接企业总部、远程办事处和分支企业，企业拥有与专用网络的相同政策，包括安全、服务质量（QoS）、可管理性和可靠性。

3. Extranet VPN

Extranet VPN 即企业间发生收购、兼并或企业间建立战略联盟后，使不同企业网通过公网来构筑的虚拟专用网。提供 B2B 电子商务之间的安全访问服务。

随着信息时代的到来，企业越来越重视各种信息的处理。希望可以提供给客户最快捷方便的信息服务，通过各种方式了解客户的需要，同时企业之间的合作关系也越来越多，信息交换日益频繁。因特网为这样的一种发展趋势提供了良好的基础，而如何利用因

特网进行有效的信息管理，是企业发展中不可避免的一个关键问题。利用 VPN 技术可以组建安全的 Extranet，既可以向客户、合作伙伴提供有效的信息服务，又可以保证自身的内部网络的安全。

Extranet VPN 对用户的吸引力在于：能容易地对外部网进行部署和管理，外部网的连接可以使用与部署内部网和远端访问 VPN 相同的架构和协议进行部署。主要的不同是接入许可，外部网的用户被许可只有一次机会连接到其合作人的网络，并且只拥有部分网络资源访问权限，这要求企业用户对各外部用户进行相应访问权限的设定。

【实验原理】

IPSec 的主要作用是为 IP 数据通信提供安全服务。IPSec 不是一个单独协议，它是一套完整的体系框架，包括 AH、ESP 和 IKE 三个协议。IPSec 使用了多种加密算法、散列算法、密钥交换方法等为 IP 数据流提供安全性，提供数据的机密性、数据的完整性、数据源认证和反重放等安全服务。

在使用 IKE 为 IPSec 提供协商机制时，可以使用两种对等体认证方式：预共享密钥和数字签名（或称数字证书），本实验使用预共享密钥认证方式。

当将 VPN 网关设置为桥接模式后接入到网络中时，无需改变编址和路由拓扑，保证了现有网络的拓扑结构，这时 IPSec VPN 隧道是建立在两个 VPN 网关的虚拟桥接接口（Bridge）之间。

【实验步骤】

第一步：准备好 PC。

准备好 PC1 和 PC2 后，先在 PC1 和 PC2 上安装 VPN 管理软件。具体的安装步骤不在这里详述，可以查看 VPN 产品的随机说品书和产品光盘。

第二步：搭建拓扑，配置 IP 地址。

按照如图 3-57 所示拓扑图，搭建实验拓扑，并根据如表 3-3 所示编址方案，配置各设备的 IP 地址。

表 3-3 设备 IP 地址

设　备	接　口	地　址
VPN 网关 A	br0 口地址	10.1.1.1
PC1	PC1 的 IP 地址	10.1.1.3
	PC1 网关地址	10.1.1.1
VPN 网关 B	br0 口地址	10.1.2.1
PC2	PC2 的 IP 地址	10.1.2.3
	PC2 网关地址	10.1.2.1
Router	F0/0 地址	10.1.1.2
	F0/1 地址	10.1.2.2

说明：PC 及 Router 地址的配置方式不再详述。

(1) 通过 PC1 超级终端,转入命令行状态,在命令行下配置 VPN 网关 A 的 br0 桥接接口地址,操作如图 3-57 所示。

```
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# bridge create
br0      Configuration:
         OnBoot Yes        Mode UnCfg
         HWAddress Unset MTU Unset        Link-Guarantee NotSupport

         Status:
         Type Unknown
         Up UnLink Half-Duplex UnknownSpeed       HWAddress 00:00:00:00:00:00
         IPAddress 0.0.0.0          NetMask 0.0.0.0
         GateWay 0.0.0.0 MTU 1500
         RX Pkts            0 Bytes            0 Errors            0 Dropped            0
         TX Pkts            0 Bytes            0 Errors            0 Dropped            0

[sadm@RG-WALL(Network)]# bridge set
Bridge to set (br0, Enter means cancel):
br0
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, Enter means Manual):
1
IP Address (xxx.xxx.xxx.xxx):
10.1.1.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.0.0.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):
10.1.1.2
MTU (68-1500, Enter means use MTU of device):

Link-Guarantee Weight (1-255, Enter means 100):

[sadm@RG-WALL(Network)]#
```

图 3-57 配置 VPN 网关 A 的 br0 桥接接口

(2) 把 eth0 接口和 eth1 接口加入到 br0 接口,操作如图 3-58 所示。

```
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth0
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):
4
Parent bridge (br0):
br0
MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):
4
Parent bridge (br0):
br0
MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]#
```

图 3-58 通过 PC1 终端把 eth0、eth1 接口加入到 br0 接口

(3) 通过 PC2 的超级终端,转入命令行状态,在命令行下配置 VPN 网关 B 的 br0 桥接接口地址,操作如图 3-59 所示。

(4) 把 eth0 接口和 eth1 接口加入到 br0 接口,操作如图 3-60 所示。

第三步:配置 VPN 网关 A 的 IPSec VPN 隧道。

(1) 进行设备配置。

打开"虚拟专用网"中"隧道配置"项,单击"添加设备"按钮,添加设备,如图 3-61 所示。

```
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# bridge create
br0      Configuration:
         OnBoot Yes      Mode UnCfg
         HWAddress Unset MTU Unset        Link-Guarantee NotSupport

         Status:
         Type Unknown
         Up UnLink Half-Duplex UnknownSpeed      HWAddress 00:00:00:00:00:00
         IPAddress 0.0.0.0        NetMask 0.0.0.0
         GateWay 0.0.0.0 MTU 1500
         RX Pkts          0 Bytes          0 Errors          0 Dropped          0
         TX Pkts          0 Bytes          0 Errors          0 Dropped          0

[sadm@RG-WALL(Network)]# bridge set
Bridge to set (br0, Enter means cancel):
br0
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, Enter means Manual):
1
IP Address (xxx.xxx.xxx.xxx):
10.1.2.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.0.0.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):
10.1.2.2
MTU (68-1500, Enter means use MTU of device):

Link-Guarantee Weight (1-255, Enter means 100):

[sadm@RG-WALL(Network)]#
```

图 3-59　配置 VPN 网关 B 的 br0 桥接接口

```
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth0
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):
4
Parent bridge (br0):
br0
MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):
4
Parent bridge (br0):
br0
MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]#
```

图 3-60　通过 PC2 终端把 eth0、eth1 接口加入到 br0 接口

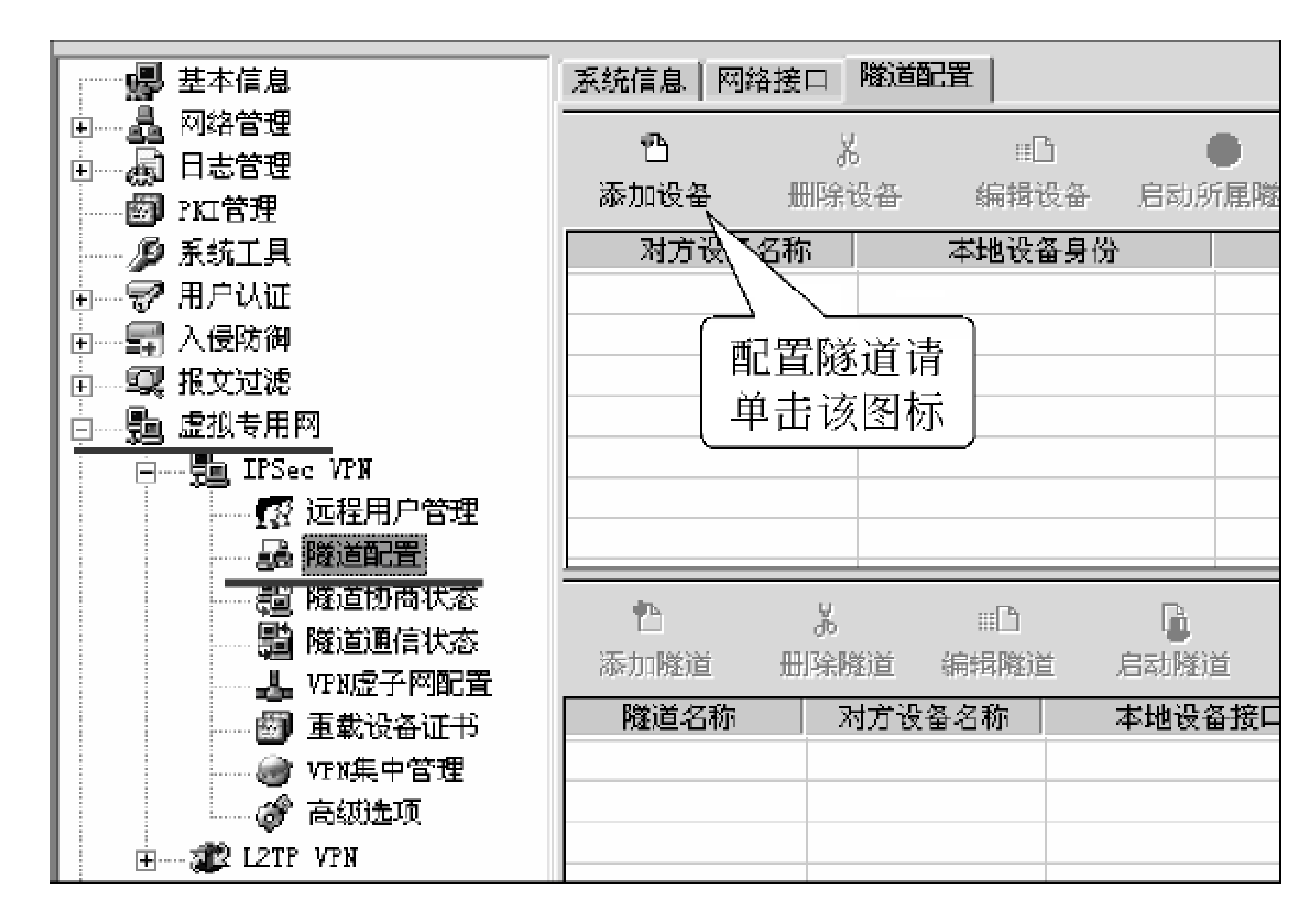


图 3-61　添加 IPSec VPN 隧道设备

在打开的 IPSec VPN 隧道“设备信息”中选择设备名称和共享密钥，如图 3-62 所示。

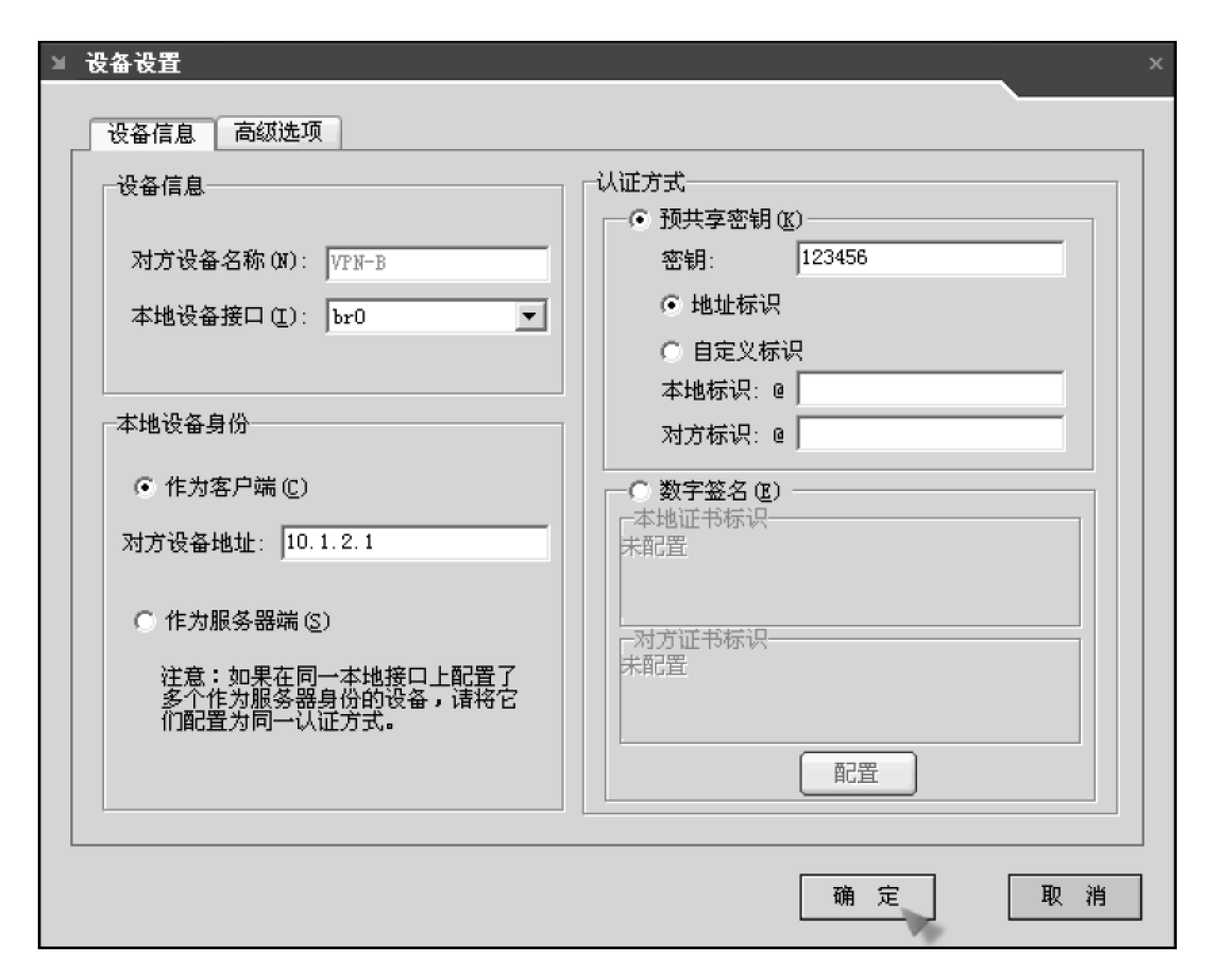


图 3-62　配置 IPSec VPN 隧道设备信息

按照图 3-63 所示内容，在隧道设备信息的“高级选项”中配置相关信息。



图 3-63　配置 IPSec VPN 隧道设备高级选项信息

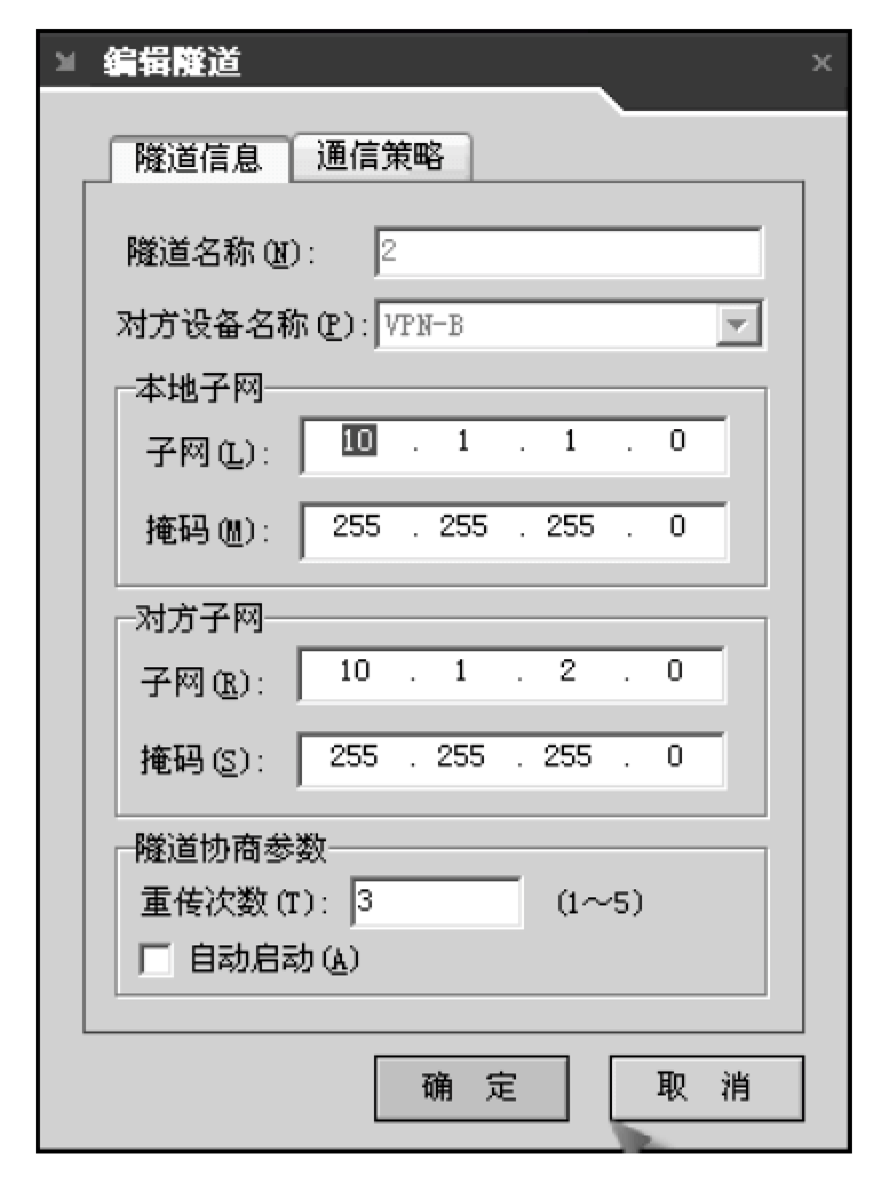
(2) 在图 3-61“隧道配置”选项中进行隧道配置，如图 3-64 所示。选择添加的设备，单击“添加隧道”按钮。



图 3-64　添加新隧道

如图 3-65 所示，在添加的新隧道中为添加隧道配置隧道信息，配置内容如图 3-65 所示。

为添加的信息隧道配置“通信策略”信息，配置的内容如图 3-66 所示。



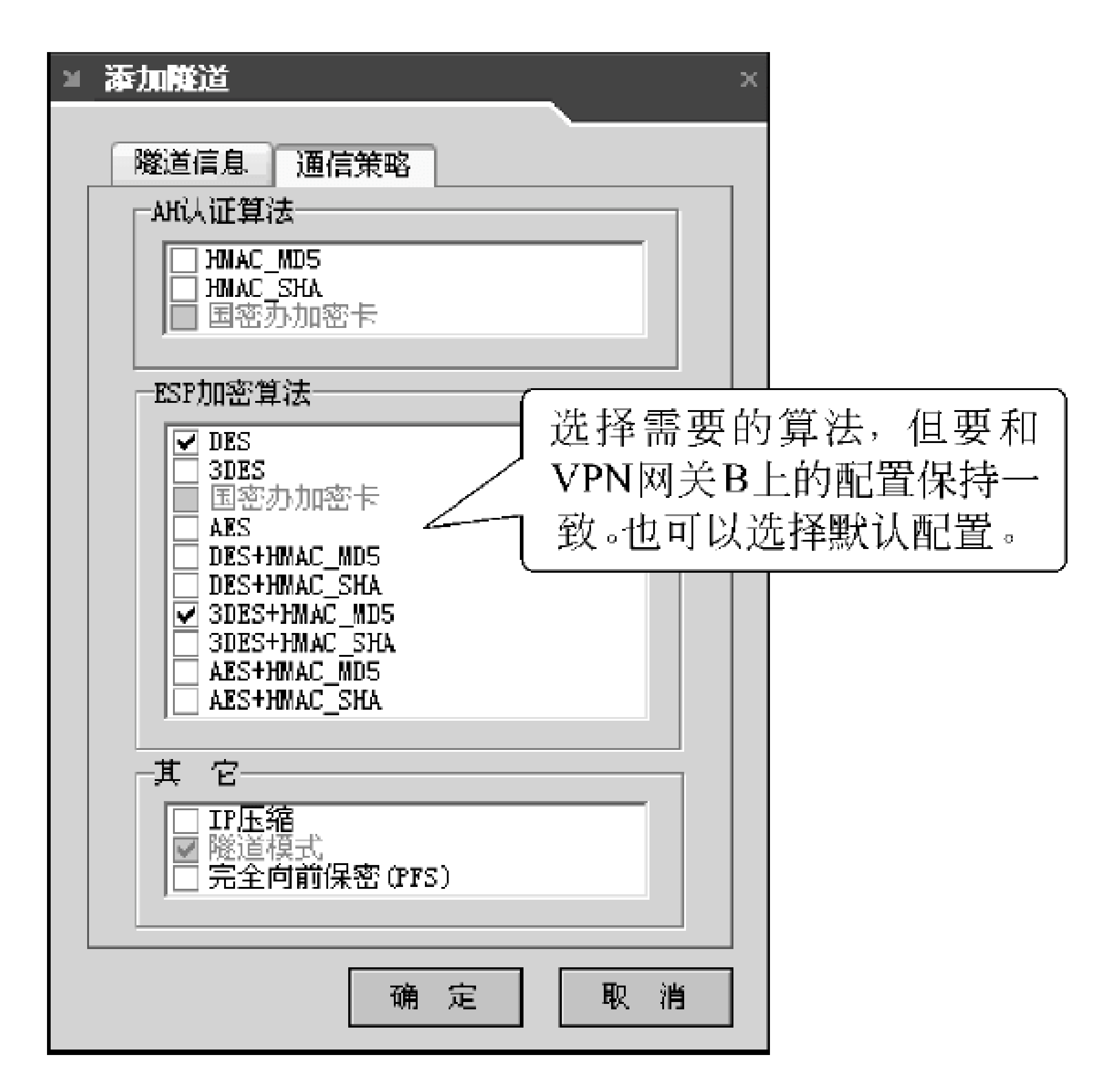



图 3-65　配置隧道信息

图 3-66　配置“通信策略”信息

第四步：配置 VPN 网关 B 的 IPSec VPN 隧道。

(1) 进行设备配置。

继续打开图 3-61“虚拟专用网”中“隧道配置”项，单击“添加设备”按钮，继续添加设备，如图 3-67 所示。

在 IPSec VPN 隧道设备信息中，选择设备名称和共享密钥，如图 3-68 所示。

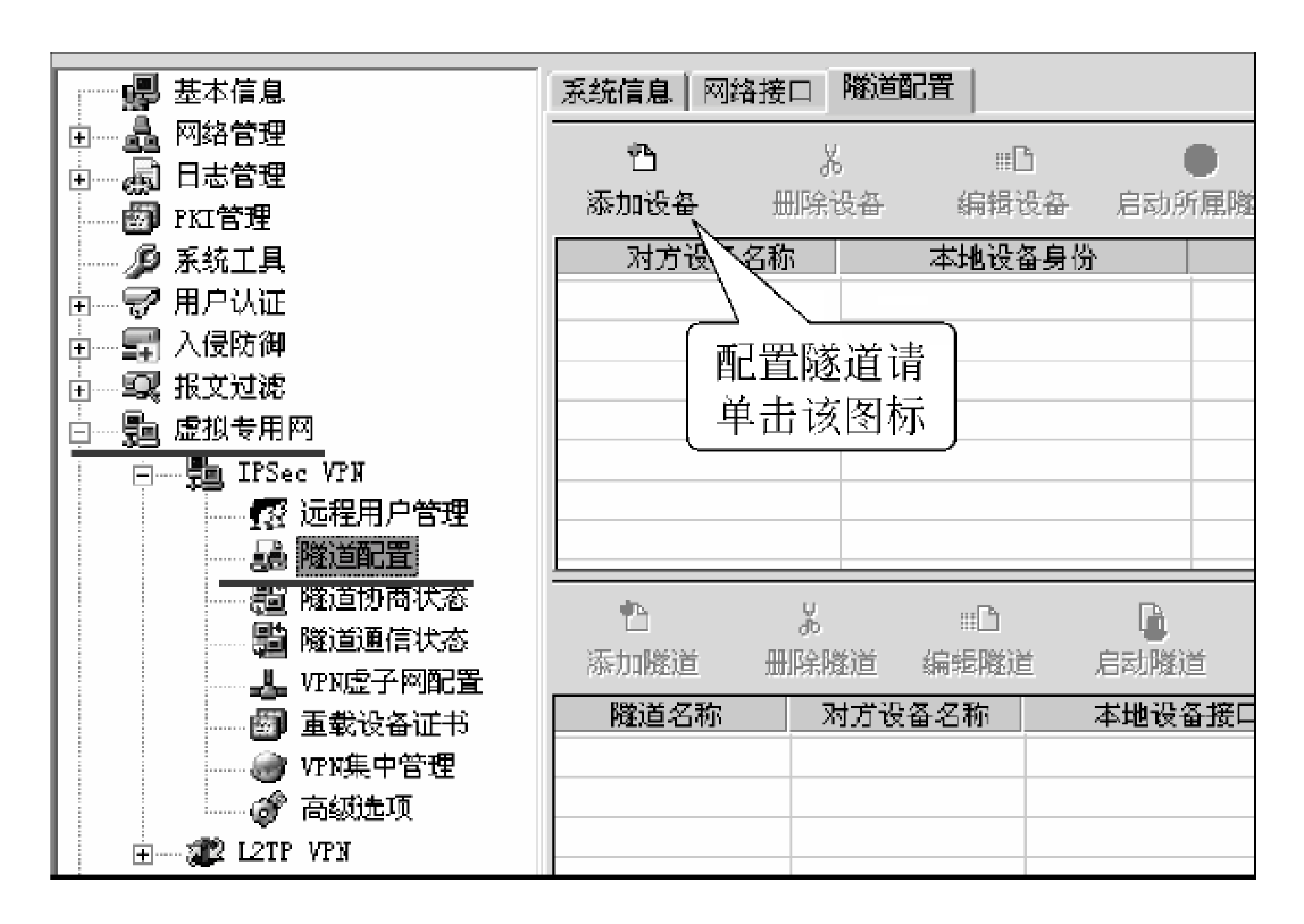


图 3-67　添加 IPSec VPN 隧道设备



图 3-68　配置 IPSec VPN 隧道设备信息

如图 3-69 所示，在隧道设备信息的“高级选项”中配置相关信息，内容如图所示。

(2) 进行隧道配置。

在“隧道配置”选项中进行隧道配置，如图 3-70 所示，选择添加的设备，单击“添加隧道”按钮进行隧道配置。

如图 3-71 所示，在添加的新隧道中为添加隧道配置隧道信息，内容如图所示。

为添加的信息隧道配置“通信策略”信息，如图 3-72 所示。

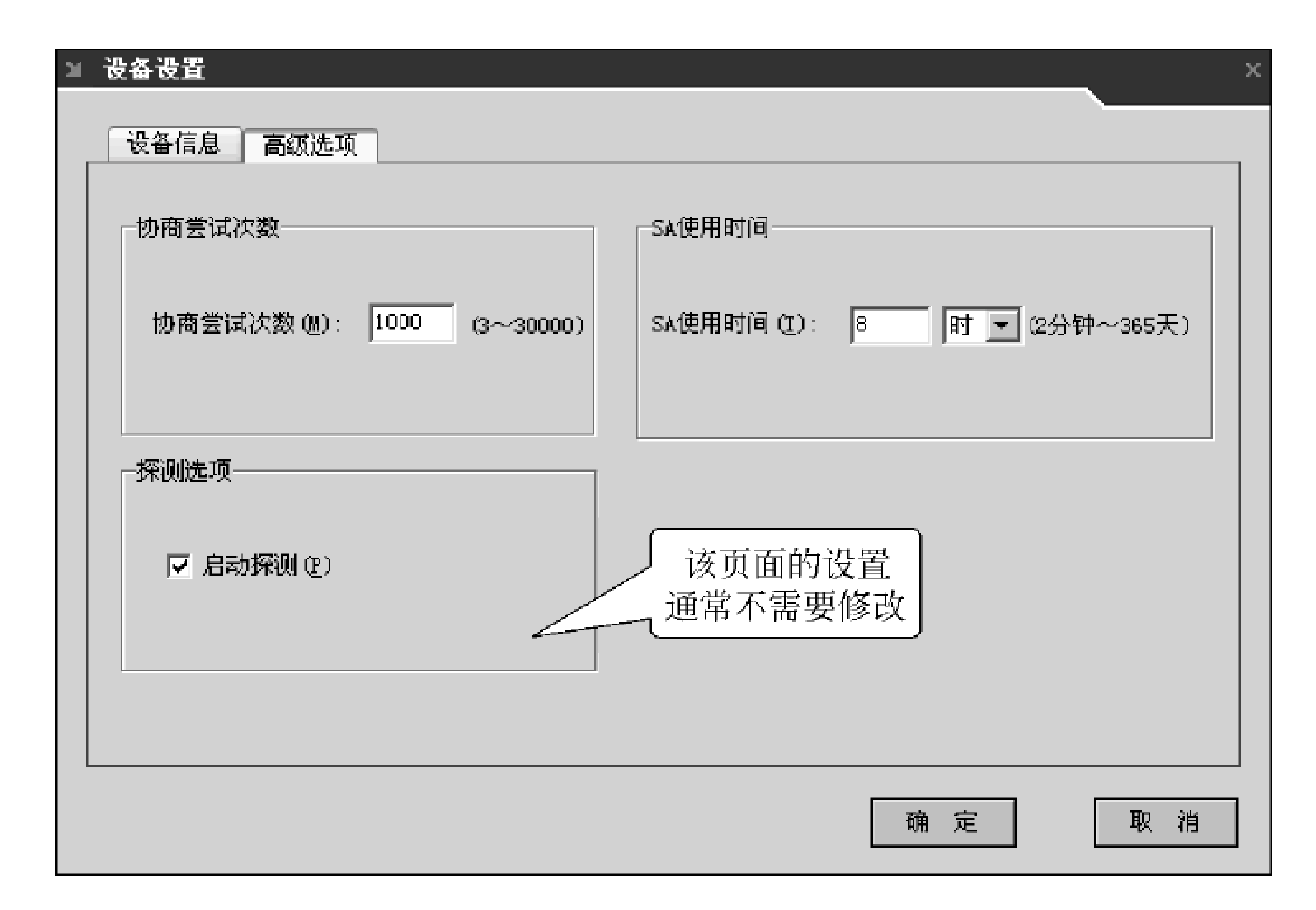


图 3-69 配置 IPSec VPN 隧道设备高级选项信息



图 3-70 添加隧道配置

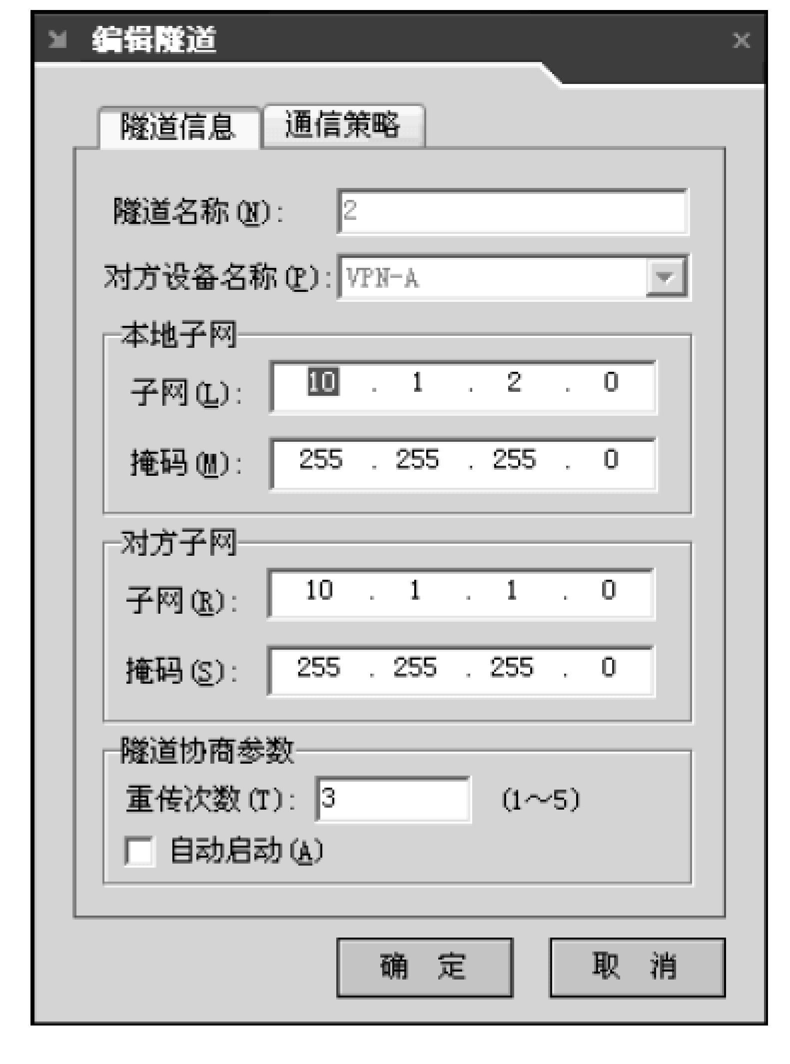


图 3-71 配置隧道信息

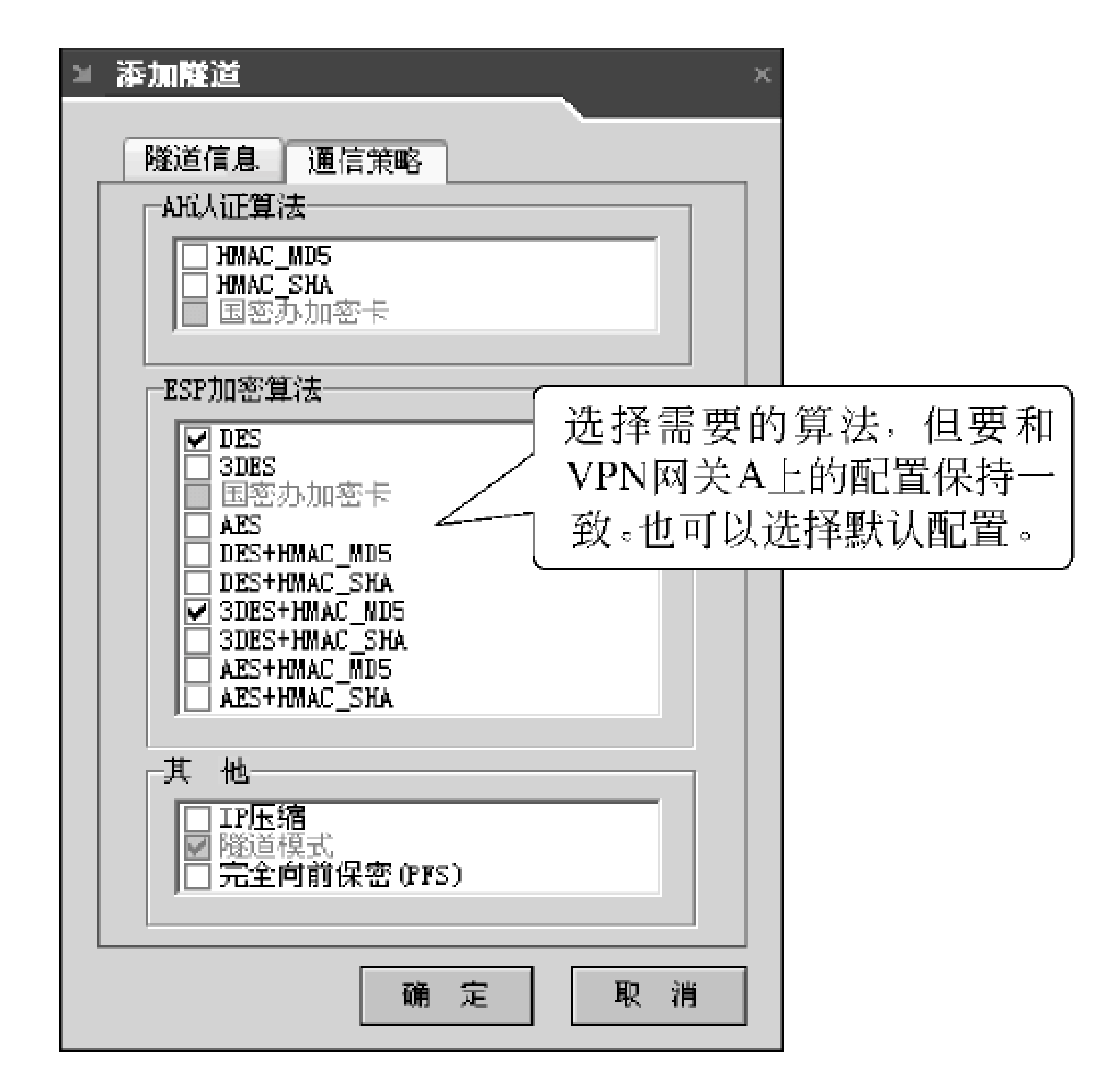


图 3-72 配置隧道“通信策略”信息

如图 3-73 所示，为添加完隧道后的界面截图。

添加隧道　删除隧道　编辑隧道　启动隧道　暂停隧道

隧道名称	对方设备名称	本地设备接口	对方设备地址	本地子网	对方子网
2	VPN-A	br0	10.1.1.1	10.1.2.0/255.255.255.0	10.1.1.0/255.255.255.0

图 3-73　配置完成隧道信息

第五步：启动隧道。

如图 3-74 所示，选择添加好隧道，单击“启动隧道”按钮，启动配置完成的隧道。

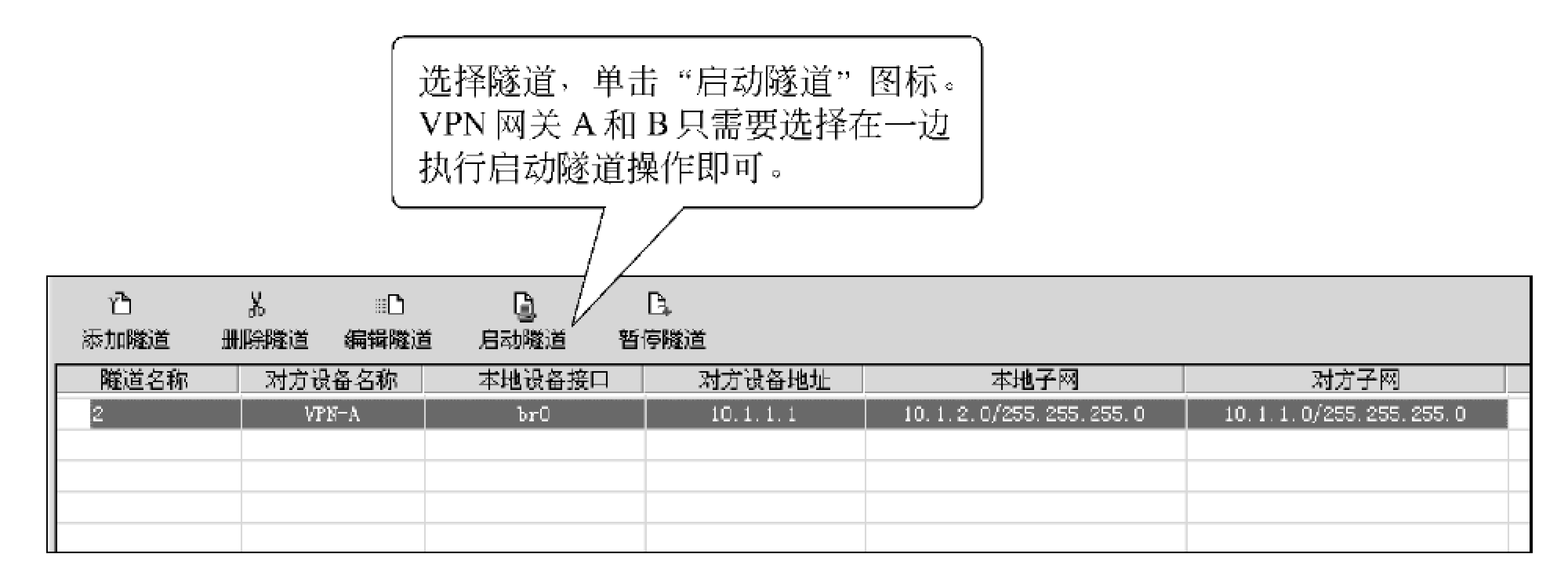


图 3-74　启动配置完成的隧道

第六步：验证测试。

隧道启动后可以在“隧道协商状态”栏下看到隧道的协商状态，如图 3-75 所示。

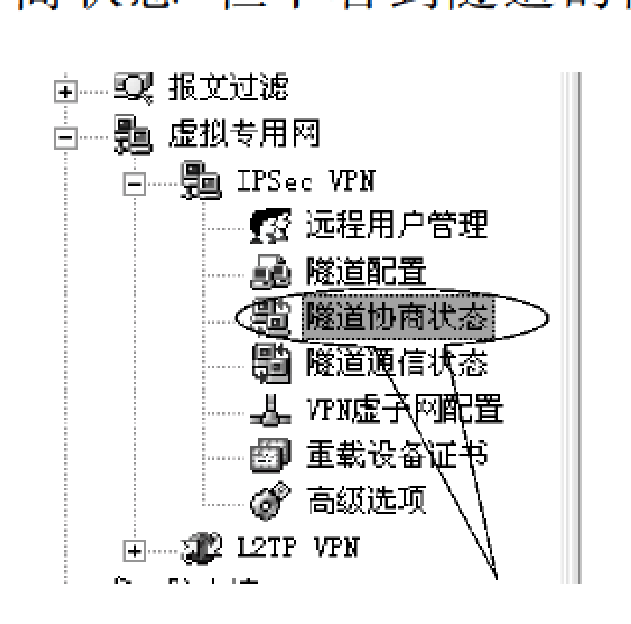


图 3-75　查看隧道的协商状态

如果协商的“隧道状态”显示“第二阶段协商成功”，则表示 VPN 网关 A 到 VPN 网关 B 的加密隧道已建立成功，如图 3-76 所示。

系统信息 | 隧道配置 | 隧道通信状态 | 隧道协商状态 | 虚子网配置

隧道协商状态　　隧道状态总数：1条

对方设备名称

序号	隧道名称	隧道状态	本地IP	对方IP	本地子网	对方子网
对方设备名称：VPN-B						
1	2	第二阶段协商成功	10.1.1.1	10.1.2.1	10.1.1.0/24	10.1.2.0/24

图 3-76　协商好的隧道信息

第七步：进行隧道通信。

VPN 隧道的通信可以是双向的，既可以从 PC1 去访问 PC2，也可以从 PC2 去访问 PC1。从 PC1 ping PC2 的地址，现在因为有了 VPN 隧道所以 ping 是可以成功的（没有 VPN 隧道前 ping 会失败），VPN 隧道的通信情况可以在“隧道通信状态”中查看到，如图 3-77 所示。

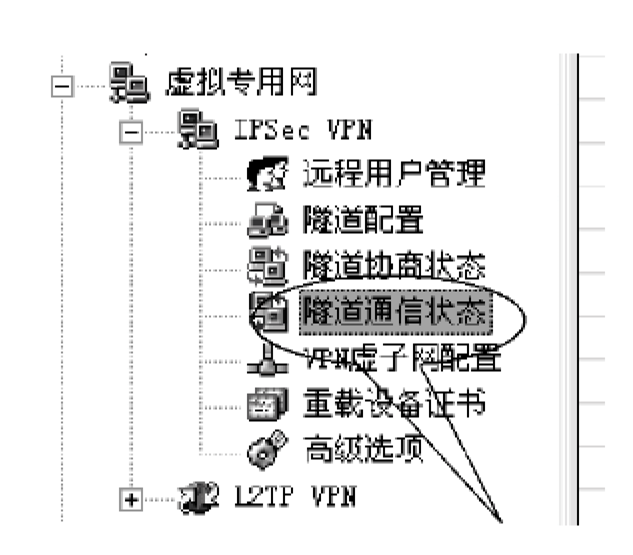


图 3-77　查看隧道通信信息

VPN 隧道的通信情况可以在“隧道通信状态”中查看到，如图 3-78 所示。

系统信息 | 隧道配置 | 隧道通信状态 | 隧道协商状态 | 虚子网配置

隧道通信状态

序号	本地子网	对方子网	发送成功包数	发送失败包数	发送成功字节数
1	10.1.1.0/24	10.1.2.0/24	9	0	540

图 3-78　VPN 隧道的通信情况

【注意事项】

- 实验环境地址可以随意定义，但请不要使用 1.1.1.0 这个网段的 IP，因为某些功能实现的需要，系统内部已占用该网段的部分 IP。
- 该实验中，VPN 网关的防火墙规则为全部开放。但在实际的网络环境中，如果 VPN 网关直接连接 Internet 网络，则一定需要启用防火墙规则。

第 4 章 基于 VPN 专用设备高级安全

4.1 在地址重叠环境中部署 IPSec VPN

【实验名称】

在地址重叠环境中部署 IPSec VPN。

【实验目的】

学习在地址重叠的情况下，构建站点到站点(Site-to-Site)的 IPSec VPN 隧道，加深对 IPSec 的理解。

【背景描述】

北京的某公司在上海设立了新的分公司，分公司要远程访问总公司内网中的各种网络资源，例如 CRM 系统、FTP 服务器等。在 Internet 上传输数据本身存在安全隐患，公司希望通过 IPSec VPN 技术实现数据的安全传输。

但目前存在的一个问题是，总公司与分公司分别在各自组网时都使用了 192.168.1.0/24 这个子网地址，这家公司希望在不改动原有编址的基础上实现 VPN 的安全通信。

【需求分析】

需求：解决上海分公司和北京总公司之间通过 Internet 进行数据传输的安全问题。

分析：IPSec VPN 技术通过隧道技术、加解密技术、密钥管理技术、认证技术等有效地保证了数据在 Internet 传输的安全性，是目前最安全、使用最广泛的 VPN 技术。因此可以通过建立 IPSec VPN 的加密隧道，实现分公司和总公司之间的安全的数据传输。在解决子网冲突的问题上，可以用虚子网的技术来实现。

【实验拓扑】

如图 4-1 所示网络拓扑，是公司在上海设立了新的分公司，分公司要远程访问总公司的各种网络资源，实现分公司和总公司之间信息共享。为解决上海分公司和北京总公司之间通过 Internet 进行数据传输的安全问题。公司希望通过 VPN 技术，有效地保证数据在 Internet 网络传输的安全问题。

目前存在的一个问题是，总公司与分公司分别在各自组网时都使用了 192.168.1.0/24 这个子网地址，这家公司希望在不改动原有编址的基础上实现 VPN 的通信，可以使用地址重叠的情况下构建站点到站点(Site-to-Site)的 IPSec VPN 隧道，实现安全通信。

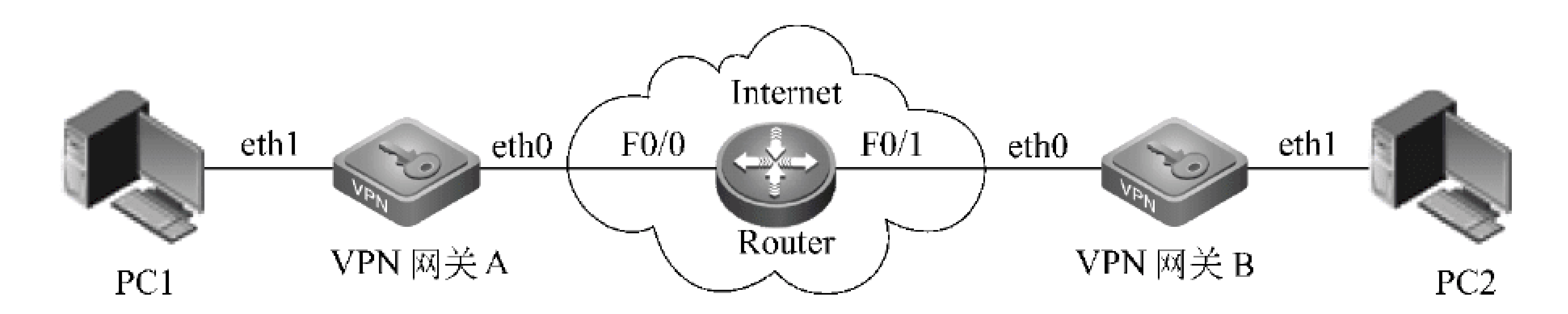


图 4-1 地址重叠环境中部署 IPSec VPN 网络拓扑

【实验设备】

RG-WALL VPN 网关:2 台;PC:2 台;路由器:1 台。

【预备知识】

IPSec 体系框架

IPSec 的主要作用是为 IP 数据通信提供安全服务,主要功能为加密和认证。为了进行加密和认证,IPSec 还需要有密钥的管理和交换功能,以便为加密和认证提供所需要的密钥,并对密钥的使用进行管理。以上三方面的工作分别由 AH、ESP 和 IKE 三个协议规定。

为了了解三个协议,需要先引入一个非常重要的术语——安全关联(Security Association,SA)。所谓安全关联是指安全服务与它服务的载体之间的一个连接,为正确封装及提取 IPSec 数据包,有必要采取一套专门的方案,将安全服务/密钥与要保护的通信数据联系到一起;同时要将远程通信实体与要交换密钥的 IPSec 数据传输联系到一起。换言之,要解决如何保护通信数据、保护什么样的通信数据以及由谁来实行保护的问题,这样的构建方案称为安全关联。

AH 和 ESP 都需要使用 SA,而 IKE 的主要功能就是 SA 的建立和维护。只要实现 AH 和 ESP 都必须提供对 SA 的支持。通信双方如果要用 IPSec 建立一条安全的传输通路,需要事先协商好将要采用的安全策略,包括使用的加密算法、密钥、密钥的生存期等。当双方协商好使用的安全策略后,就说双方建立了一个安全关联 SA。SA 就是能向其上层的数据传输提供某种 IPSec 安全保障的一个简单连接,可以由 AH 或 ESP 协议提供。当给定了一个安全关联 SA,就确定了 IPSec 要执行的处理,如加密、认证等。SA 可以进行两种方式的组合,分别为传输临近和嵌套隧道。

1. ESP

ESP(Encapsulating Secuity Payload)协议主要用来处理对 IP 数据包的加密,此外对认证也提供某种程度的支持。ESP 与具体的加密算法相独立,几乎可以支持各种对称密钥加密算法,例如 DES、TripleDES、RC5 等。为了保证各种 IPSec 实现间的互操作性,目前 ESP 必须提供对 56 位 DES 算法的支持。

ESP 协议数据单元格式由三个部分组成,除了头部、加密数据部分外,在实施认证时还包含一个可选尾部。头部有两个域:安全策略索引(SPI)和序列号(sequence number)。使用 ESP 进行安全通信之前,通信双方需要先协商好一组将要采用的加密策略,包括使用的算法、密钥以及密钥的有效期等。"安全策略索引"便用来标识发送方是使

用哪组加密策略来处理 IP 数据包的，当接收方看到了这个序号就知道了对收到的 IP 数据包应该如何处理。“序列号”用来区分使用同一组加密策略的不同数据包。加密数据部分除了包含原 IP 数据包的有效负载，填充域(用来保证加密数据部分满足块加密的长度要求)，还包含其余部分，在传输时都加密过。其中“下一个头部(Next Header)”用来指出有效负载部分使用的协议，可能是传输层协议(TCP 或 UDP)，也可能还是 IPSec 协议(ESP 或 AH)。

通常 ESP 可以作为 IP 的有效负载进行传输，其中 IP 的头部使用 UKB 单元信息指出下一个协议是 ESP，而非 TCP 和 UDP。由于采用了这种封装形式，所以 ESP 可以使用旧有的网络进行传输。

前面已经提到用 IPSec 进行加密是可以有两种工作模式，意味着 ESP 协议有两种工作模式：传输模式(Transport Mode)和隧道模式(Tunnel Mode)。当 ESP 工作在传输模式时，采用当前的 IP 头部。而在隧道模式时，将整个 IP 数据包进行加密作为 ESP 的有效负载，并在 ESP 头部前增添以网关地址为源地址的新的 IP 头部，此时可以起到 NAT 的作用。

2. AH

IPSec 认证头协议 AH(IPSec AH)是 IPSec 体系结构中的一种主要协议，它为 IP 数据报提供无连接传输的完整性与数据源认证服务，并提供保护以避免重播情况。一旦建立安全连接，接收方就可能会选择后一种服务。AH(Authentication Header)尽可能为 IP 头和上层协议数据提供足够多的认证。但是在传输过程中某些 IP 头字段会发生变化，且发送方无法预测数据包到达接受端时此字段的真正值。AH 并不能保护这种字段值变化。因此 AH 提供给 IP 头的保护有些不完善。

AH 可被独立使用，或与 IP 封装安全负载协议(ESP)结合使用，或通过使用隧道模式的嵌套方式配合使用。在通信主机与通信主机之间、通信安全网关与通信安全网关之间或安全网关与主机之间可以提供安全服务。

AH 协议只涉及认证，不涉及加密。AH 虽然在功能上和 ESP 有些重复，但 AH 除了对 IP 的有效负载进行认证外，还可以对 IP 头部实施认证。主要是处理数据对，可以对 IP 头部进行认证，而 ESP 的认证功能主要是面对 IP 的有效负载。为其提供最基本的功能并保证互操作性，AH 必须包含对 HMAC-SHA 和 HMAC-MD5(HMAC 是一种 SHA 和 MD5 都支持的对称式认证系统)的支持。

3. IKE

IKE(Internet Key Exchange)协议主要是对密钥交换进行管理，它主要包括三个功能：对使用的协议、加密算法和密钥进行协商；方便的密钥交换机制(这可能需要周期性的进行)；跟踪对以上这些约定的实施。

【实验原理】

IPSec 的主要作用是为 IP 数据通信提供安全服务。IPSec 不是一个单独协议，它是一套完整的体系框架，包括 AH、ESP 和 IKE 三个协议。IPSec 使用了多种加密算法、散列算法、密钥交换方法等为 IP 数据流提供安全性，它可以提供数据的机密性、数据的完整

性、数据源认证和反重放等安全服务。

在使用 IKE 为 IPSec 提供协商机制时，可以使用两种对等体认证方式：预共享密钥和数字签名（或称数字证书），本实验使用预共享密钥认证方式。

【实验步骤】

第一步：准备好 PC。

准备好 PC1 和 PC2 后，先在 PC1 和 PC2 上安装 VPN 管理软件。具体的安装步骤不在这里详述，可以查看产品的随机说品书和产品光盘。

第二步：搭建拓扑，配置 IP 地址。

按照如图 4-1 所示拓扑图，搭建实验拓扑，并根据如表 4-1 所示编址方案，配置各设备的 IP 地址。

表 4-1　设备 IP 地址

设　　备	接　　口	地　　址
VPN 网关 A	eth1 接口地址	192.168.1.1
	eth0 接口地址	10.1.1.1
PC1	PC1 的 IP 地址	192.168.1.2
	PC1 网关地址	192.168.1.1
VPN 网关 B	eth1 口地址	192.168.2.1
	eth0 口地址	10.1.2.1
PC2	PC2 的 IP 地址	192.168.2.2
	PC2 网关地址	192.168.2.1
Router	F0/0 地址	10.1.1.2
	F0/1 地址	10.1.2.2

说明：PC 及 Router 地址的配置方式不再详述。

（1）通过 PC1 的超级终端，在命令行状态下配置 VPN 网关 A 的 eth1 口地址，操作如图 4-2 所示。

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manu
al):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.1.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# _
```

图 4-2　配置 VPN 网关 A 的 eth1 口地址

(2) 通过 PC1 上的 VPN 管理软件,登录 VPN 网关 A,在管理界面上,选择"网络接口"项,在右侧打开窗口中,选择"eth0 口"图标,然后配置 eth0 口地址,操作如图 4-3 所示。



图 4-3　配置 eth0 口地址(1)

在打开的对话框中设置 eth0 口地址,如图 4-4 所示。

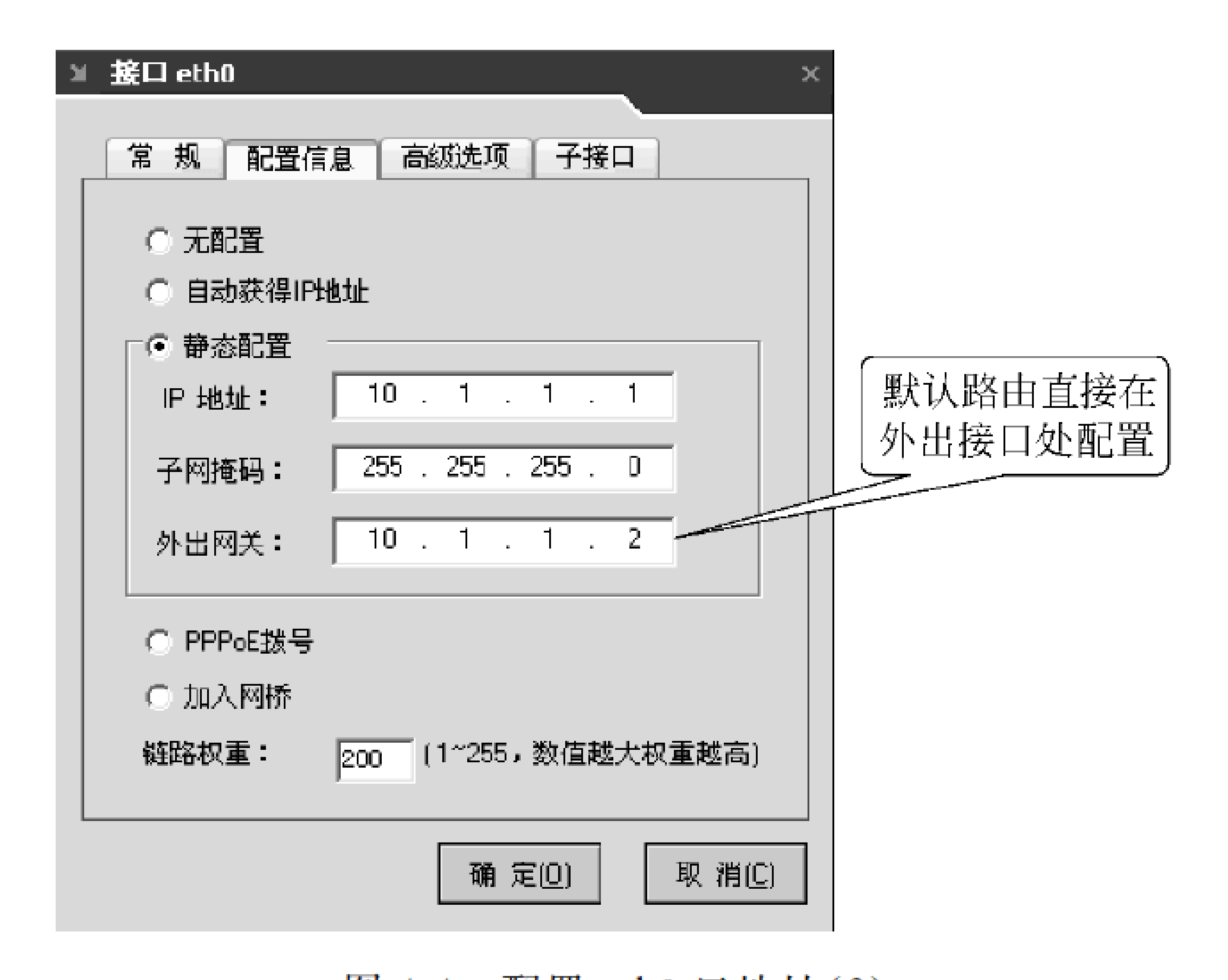


图 4-4　配置 eth0 口地址(2)

(3) 通过 PC2 的超级终端,在命令行状态下配置 VPN 网关 B 的 eth1 口地址,操作如图 4-5 所示。

(4) 通过 PC2 上 VPN 管理软件,登录 VPN 网关 B,然后在管理界面上选择"网络接口"项,在右侧打开窗口中选择"eth1 口"图标,然后配置 eth1 口地址,操作如图 4-6 所示。

在打开的对话框中设置 eth1 口地址,如图 4-7 所示。

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manu
al):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.2.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# _
```

图 4-5　命令行模式配置 VPN 网关 eth1 口地址

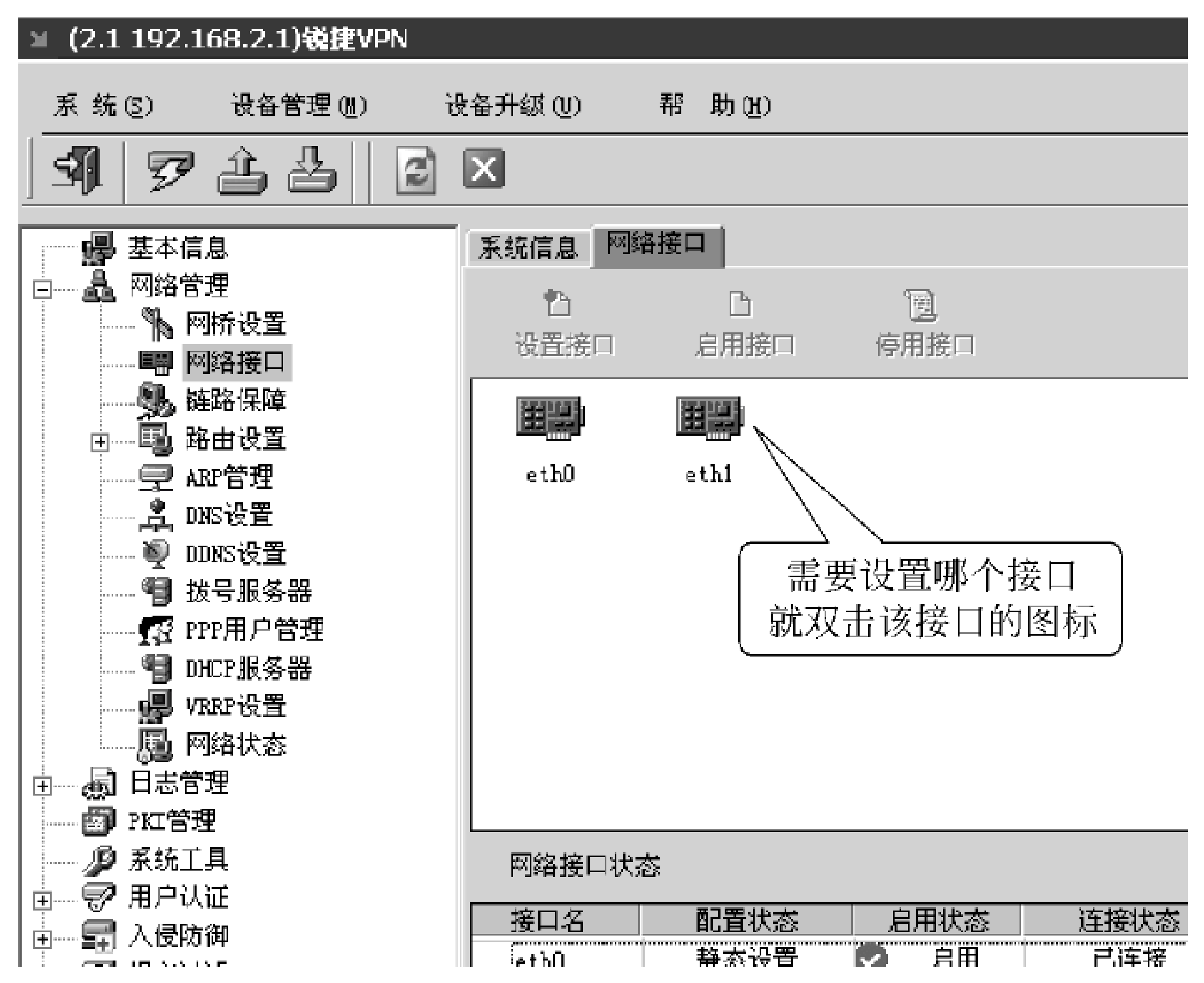


图 4-6　配置 eth1 口地址(1)



图 4-7　配置 eth1 口地址(2)

第三步：配置 VPN 网关 A 的 IPSec VPN 隧道。

(1) 配制 VPN 虚拟子网。

打开“虚拟专用网”中“VPN 虚子网配置”项，单击“添加虚子网”按钮，配置 VPN 虚子网，如图 4-8 所示。



图 4-8　配置 VPN 虚子网

在打开的配置 VPN“虚子网”对话框中，将 192.168.1.0 实子网段映射成 192.168.10.0 虚网段，如图 4-9 所示。

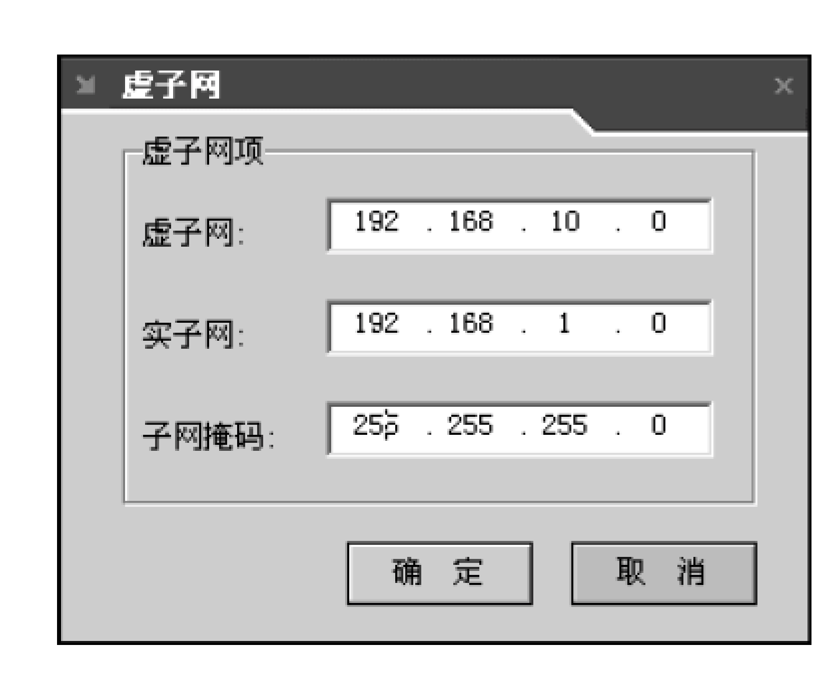


图 4-9　映射虚子网网段

(2) 进行设备配置。

打开“虚拟专用网”中“隧道配置”项，单击“添加设备”按钮，添加隧道设备，如图 4-10 所示。

在 IPSec VPN 隧道“设备配置”对话框中，选择设备名称、设备地址和认证方式，配置如图 4-11 所示信息内容。

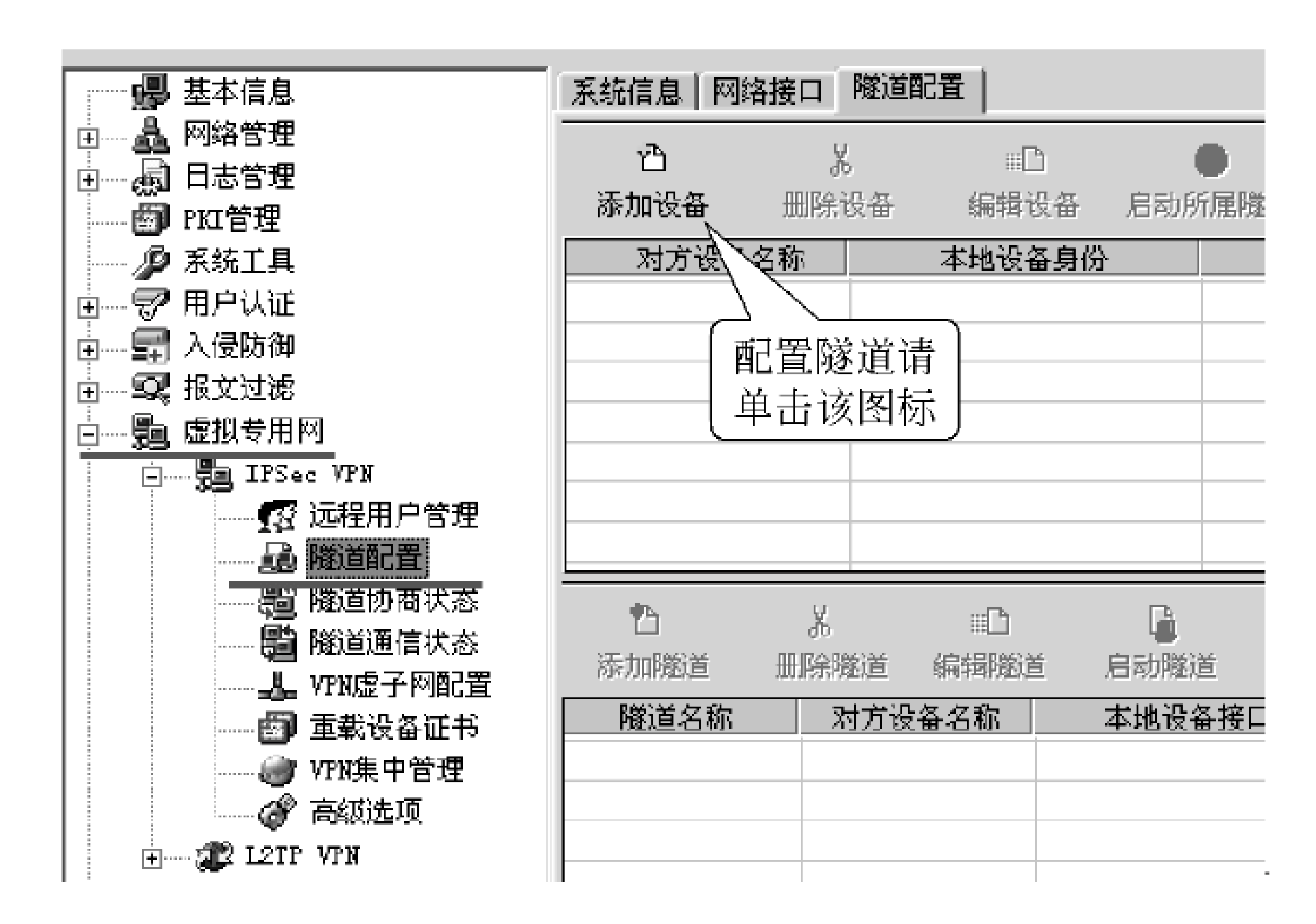


图 4-10　添加隧道设备



图 4-11　配置 IPSec VPN 隧道设备信息

如图 4-12 所示，选择隧道设备信息的“高级选项”中配置如图所示相关信息。



图 4-12　配置 IPSec VPN 隧道设备高级选项信息

(3) 进行隧道配置。

在“隧道配置”选项中进行隧道配置，如图 4-13 所示，选择添加的设备，单击“添加隧道”按钮。

如图 4-14 所示，在添加的新隧道中为添加隧道配置隧道信息。

为添加的隧道配置“通信策略”信息，如图 4-15 所示。

添加完隧道后的界面截图如图 4-16 所示。



图 4-13　添加新隧道

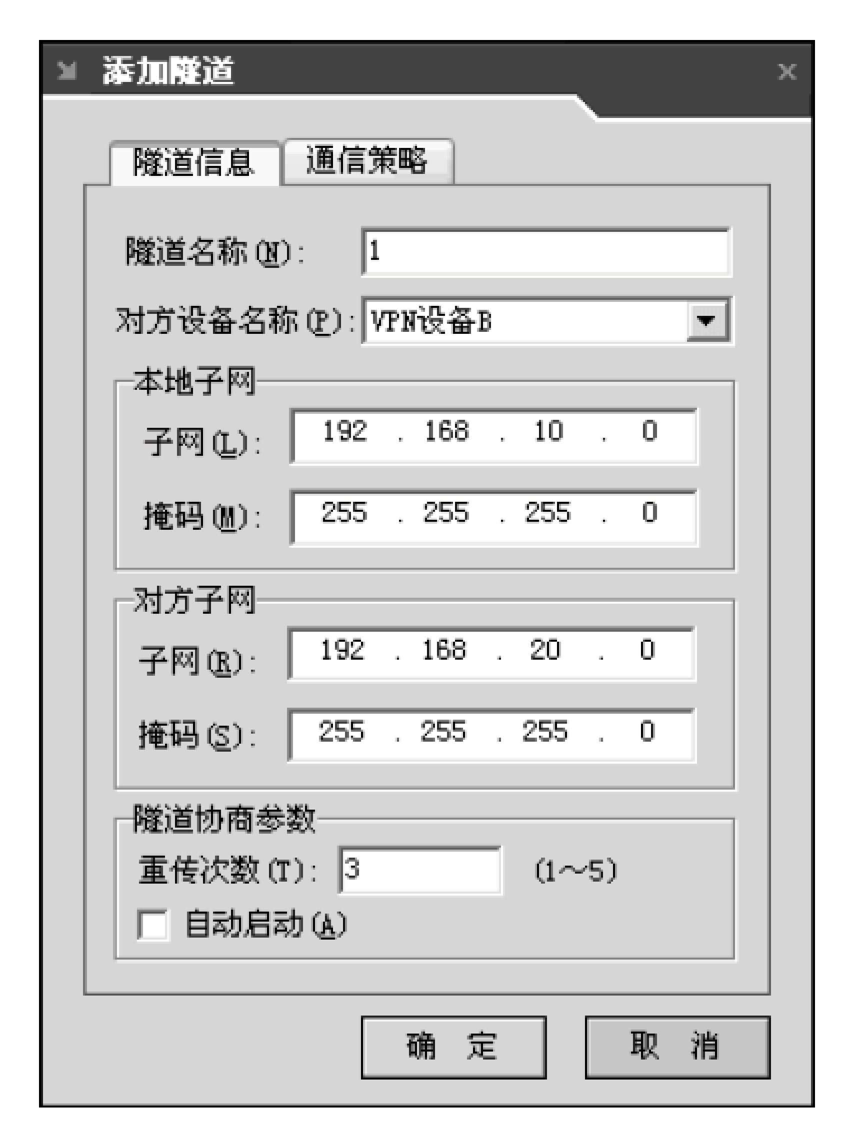


图 4-14　配置隧道信息

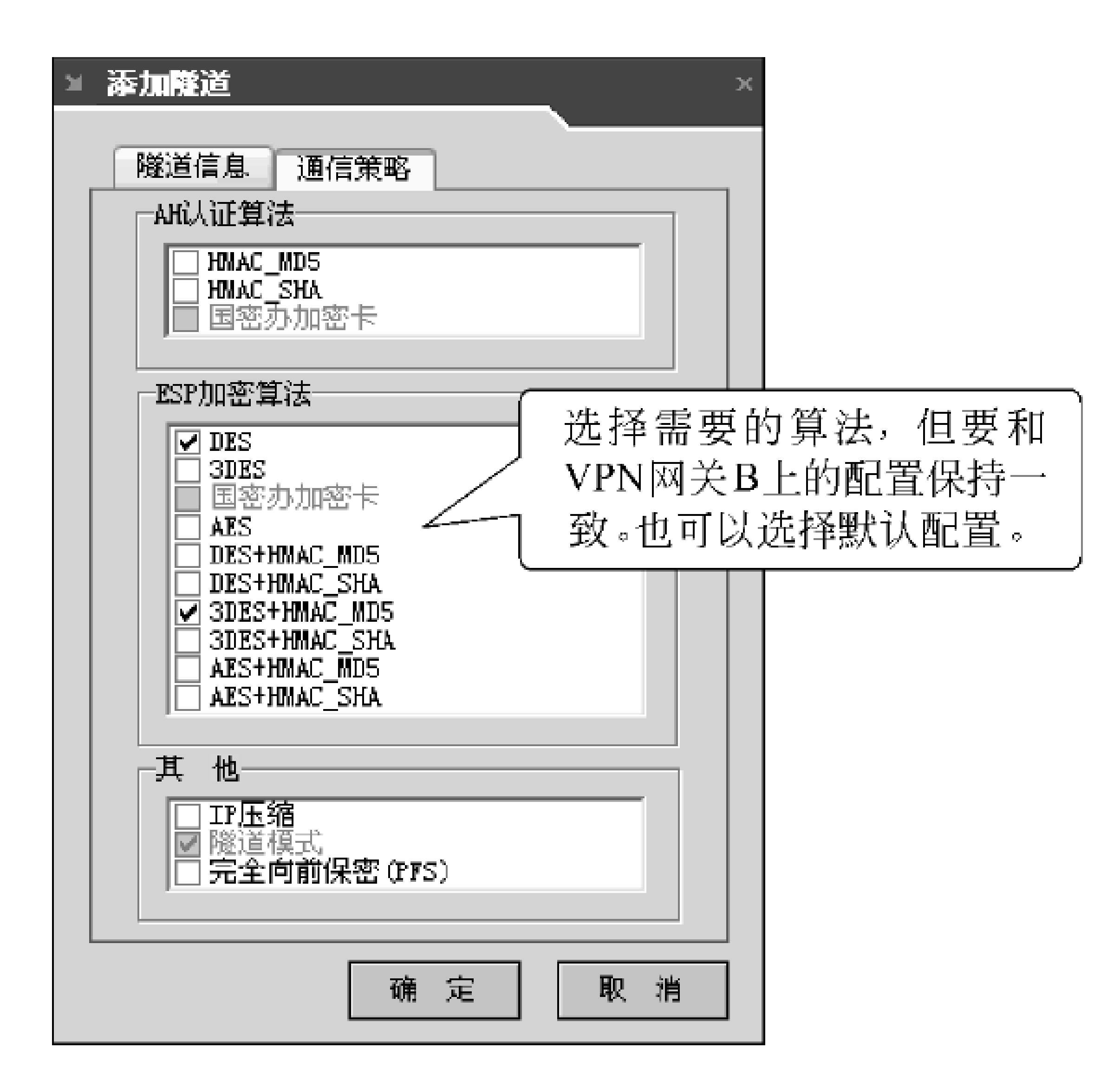


图 4-15　配置“通信策略”信息



图 4-16　完成隧道配置信息

第四步：配置 VPN 网关 B 的 IPSec VPN 隧道。

(1) 配制 VPN 虚拟子网。

打开“虚拟专用网”中“VPN 虚子网配置”项，选择相应页面上的“虚子网配置”项，单击“添加虚子网”按钮，配置 VPN 虚子网，如图 4-17 所示。



图 4-17　配置 VPN 虚子网

在打开的配置 VPN“虚子网”对话框中，将 192.168.1.0 实子网段映射成 192.168.20.0 虚网段，如图 4-18 所示。



图 4-18　映射虚子网网段

(2) 进行设备配置。

打开“虚拟专用网”中“隧道配置”项，选择对应右侧页面上的“隧道配置”项，单击“添加设备”按钮，添加隧道设备，如图 4-19 所示。

在打开 IPSec VPN 隧道“设备设置”配置信息中，选择设备名称、设备地址和认证方式，如图 4-20 所示。

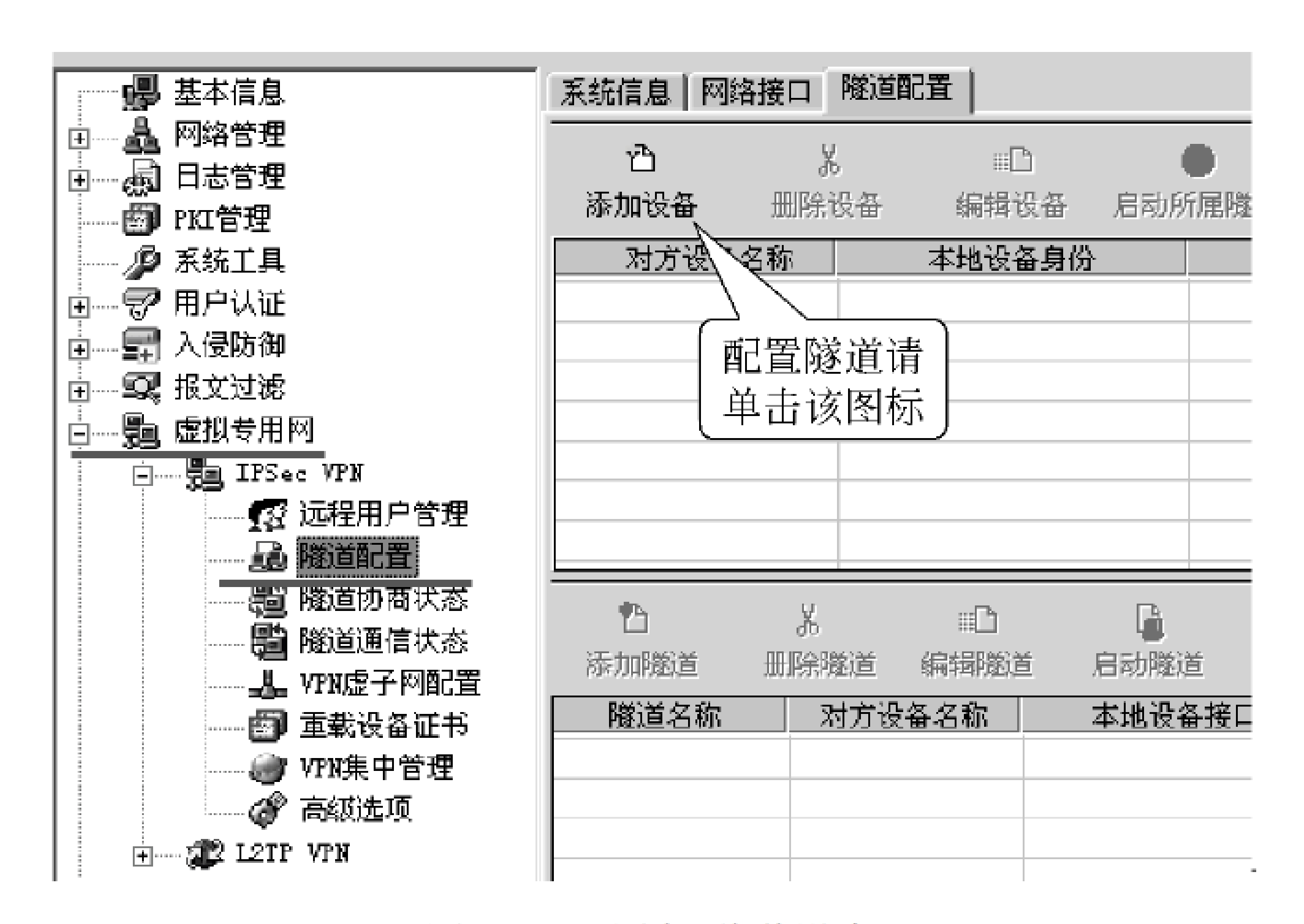


图 4-19　添加隧道设备

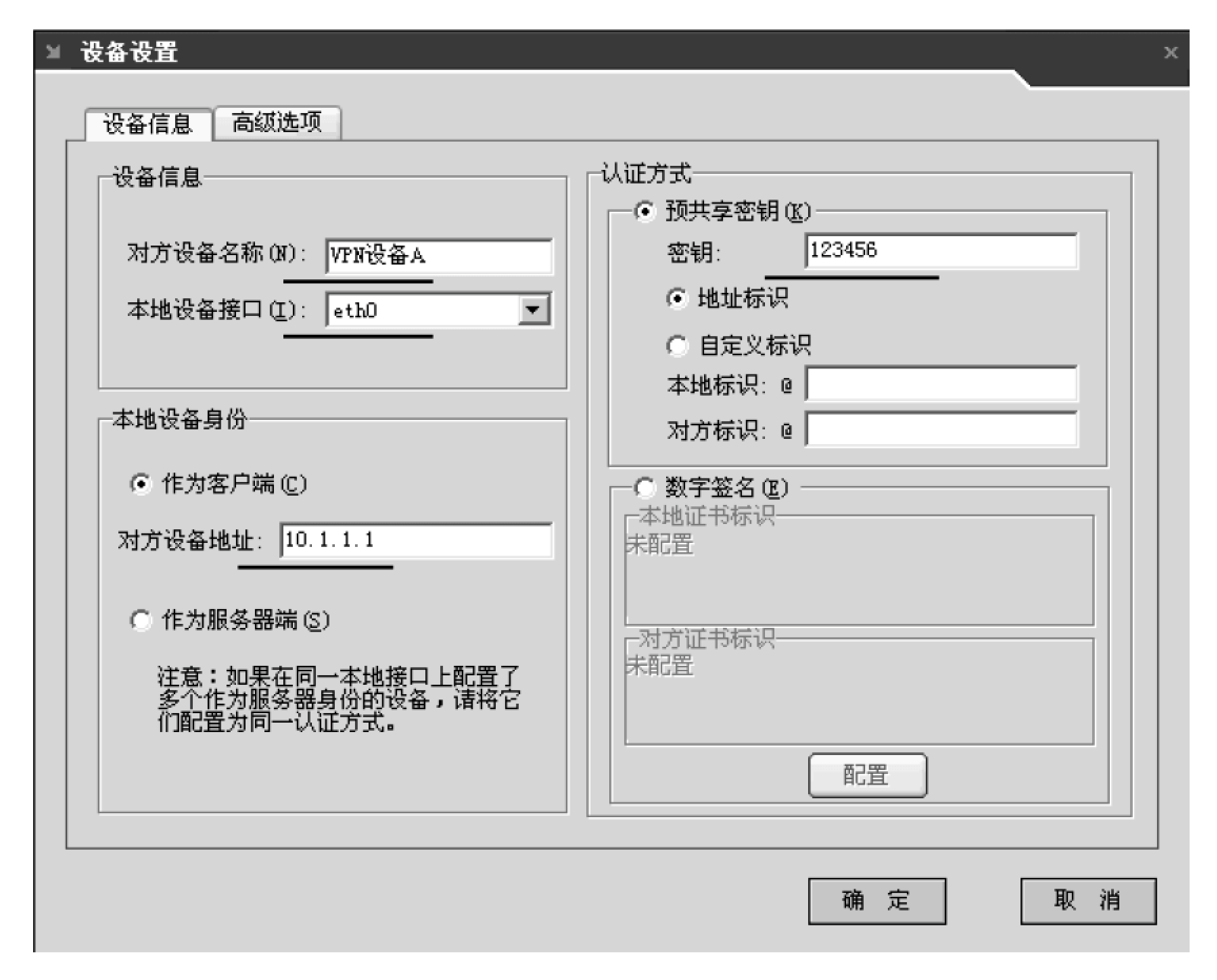


图 4-20　配置 IPSec VPN 隧道设备信息

如图 4-21 所示，在隧道设备信息的“高级选项”中配置如图所示的相关信息。

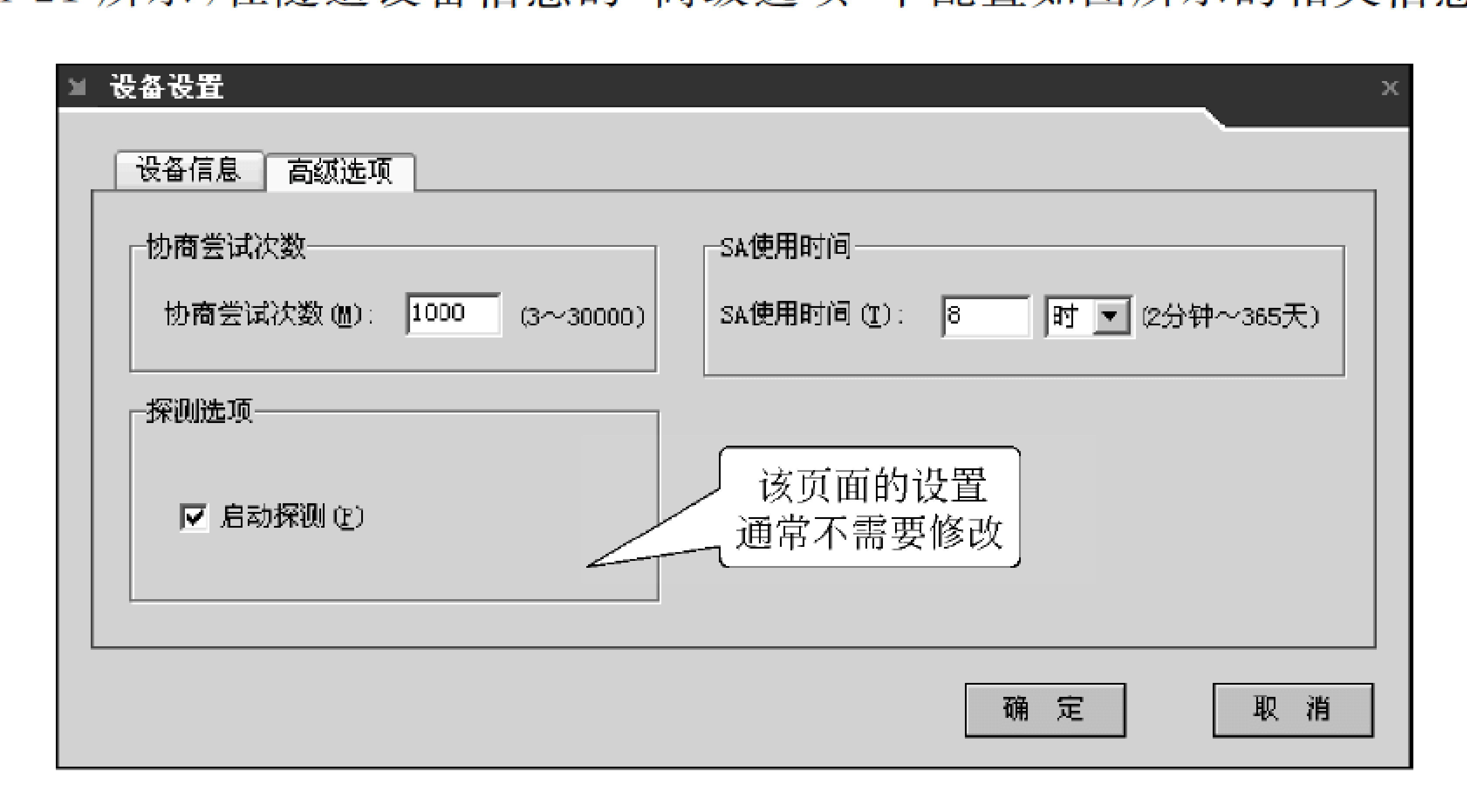


图 4-21　配置 IPSec VPN 隧道设备高级选项信息

(3) 进行隧道配置。

在图 4-19“隧道配置”选项中，继续进行隧道配置，如图 4-22 所示，选择添加的设备，单击“添加隧道”按钮。如图 4-23 所示，在添加的新隧道中，为添加隧道配置隧道信息，配置内容如图所示。

继续为添加的隧道配置“通信策略”信息，如图 4-24 所示。

添加完隧道后的界面截图如图 4-25 所示。



图 4-22 添加新隧道



图 4-23 配置隧道信息

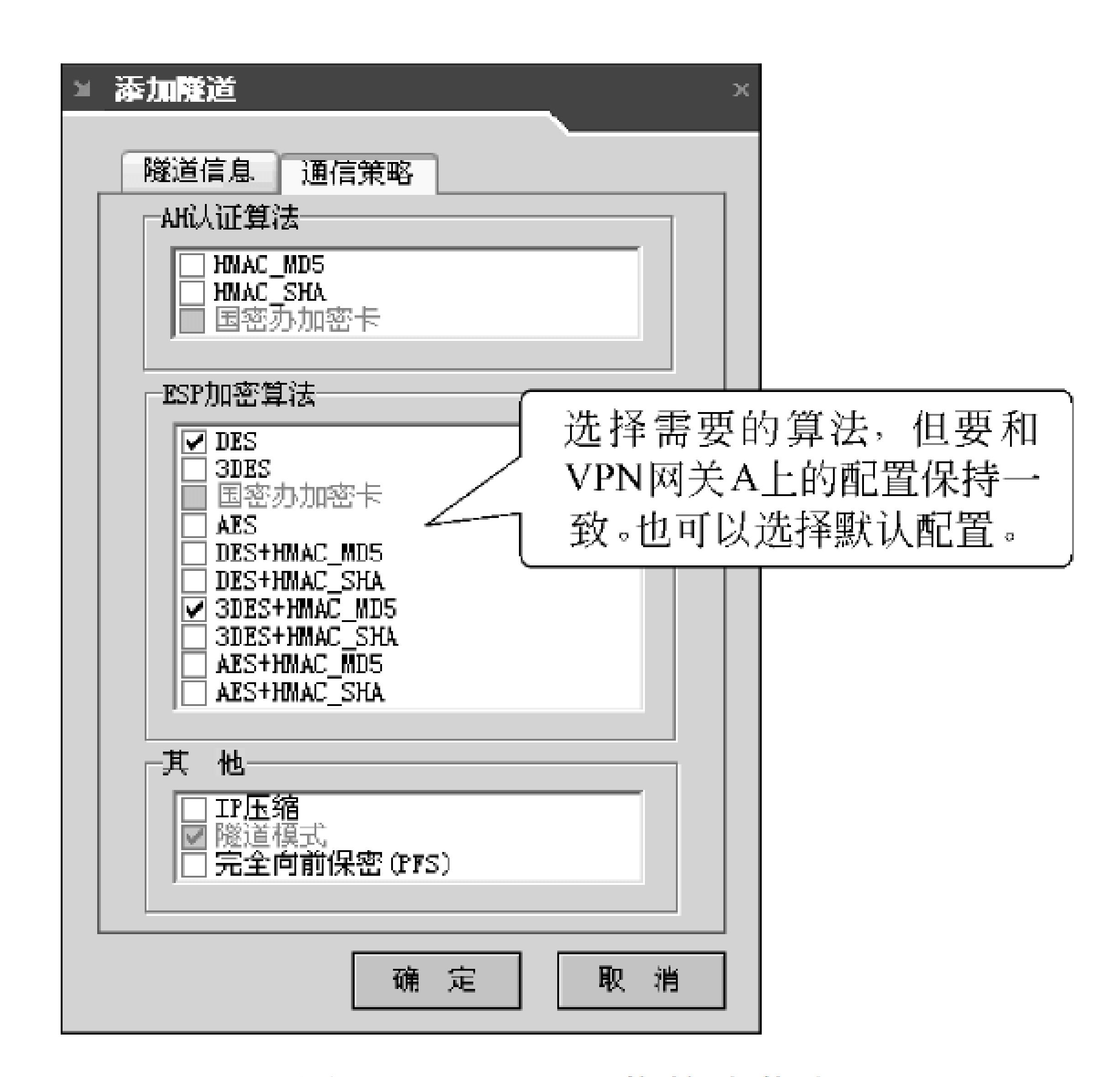


图 4-24 配置通信策略信息



图 4-25 添加完隧道信息

第五步：启动隧道。

如图 4-26 所示，选择添加好隧道，按“启动隧道”按钮，启动配置完成的隧道。VPN 网关 A 和 B 只需要选择在一边执行启动隧道操作即可。

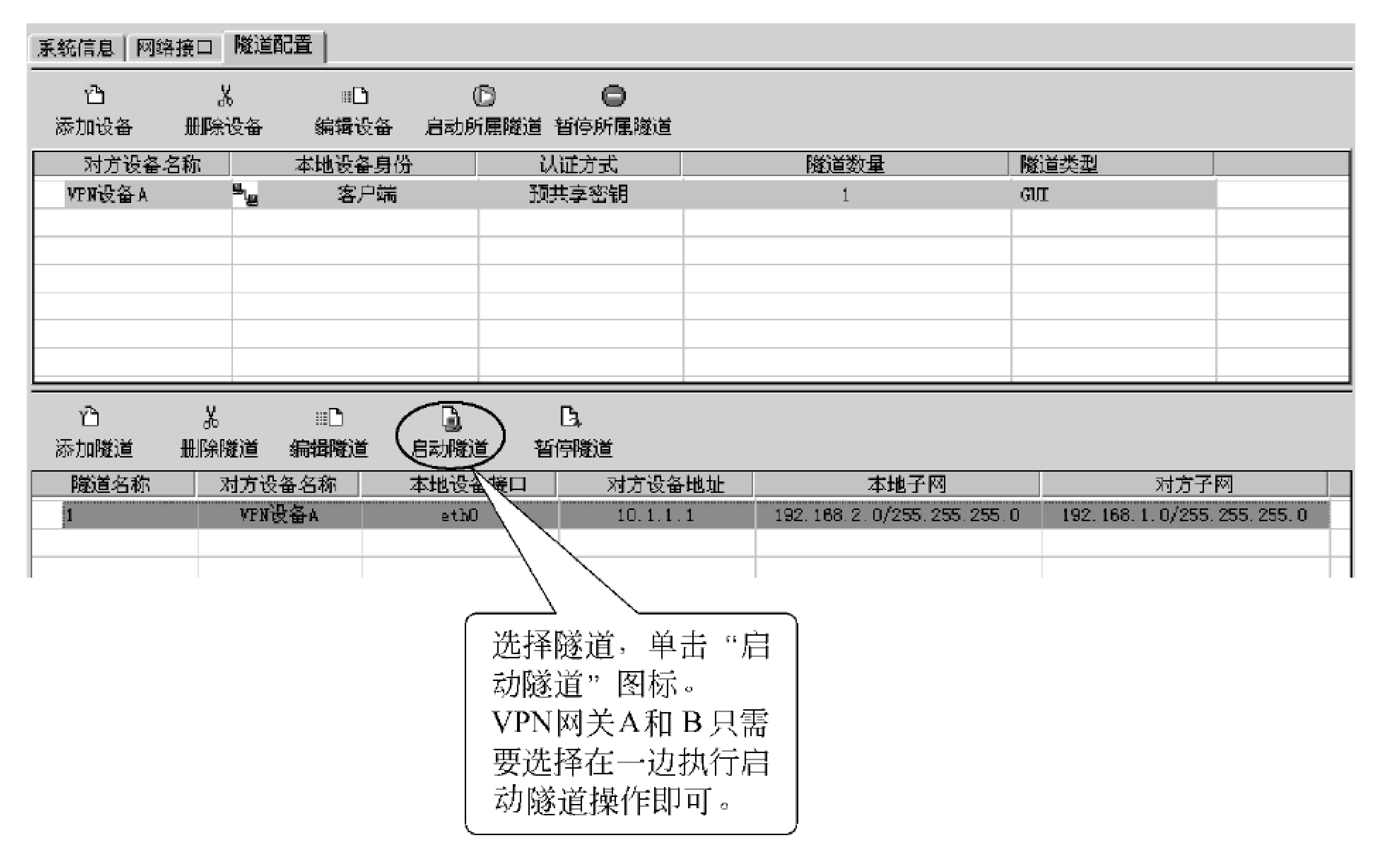


图 4-26　启动配置完成的隧道

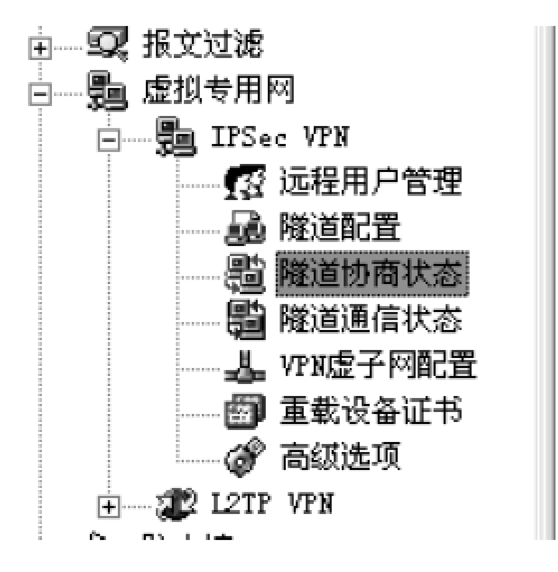


图 4-27　查看隧道的协商状态

第六步：验证测试。

隧道启动后可以在“隧道协商状态”栏下看到隧道的协商状态。如果协商的“隧道状态”显示“第二阶段协商成功”，则表示 VPN 网关 A 到 VPN 网关 B 的加密隧道已建立成功，如图 4-27 所示。

如图 4-28 所示信息，为配置完成协商好的隧道信息描述。

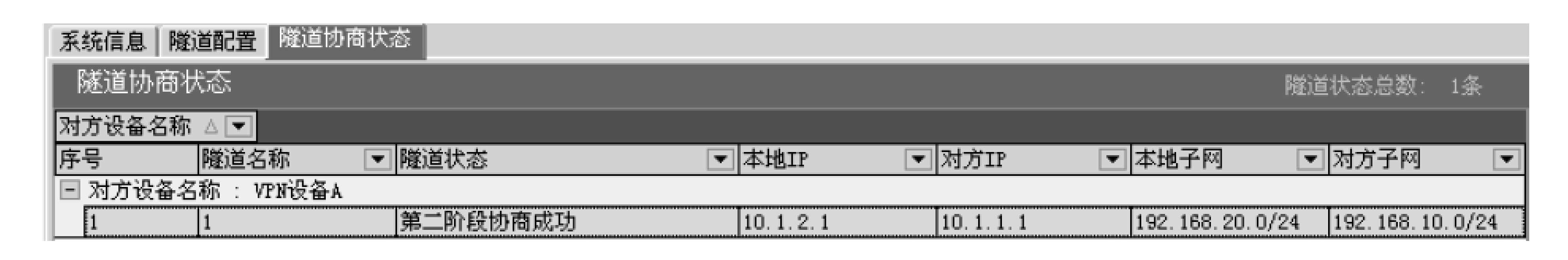


图 4-28　协商好的隧道信息

第七步：进行隧道通信。

VPN 隧道的通信是可以双向的，因此既可以从 PC1 去访问 PC2，也可以从 PC2 去访问 PC1。

从 PC1 ping PC2 的地址，现在因为有了 VPN 隧道所以 ping 是可以成功的（没有 VPN 隧道前 ping 会是失败的）。VPN 隧道的通信情况可以在“隧道通信状态”中查看到，如图 4-29 所示信息。

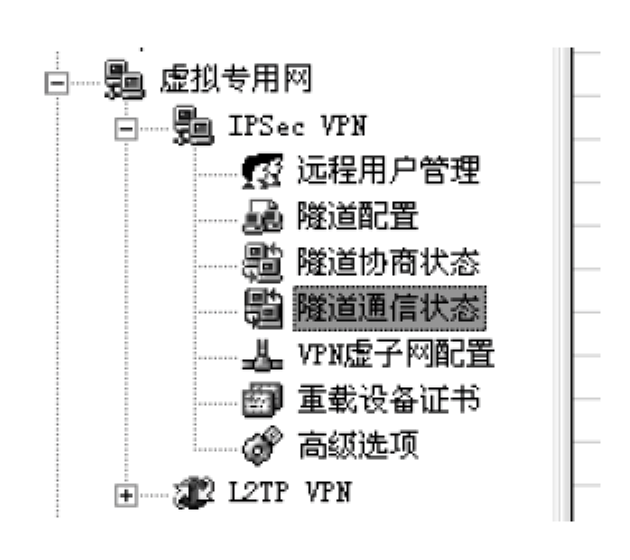


图 4-29　查看隧道通信信息

VPN 隧道的通信情况可以在"隧道通信状态"中查看到，如图 4-30 所示。

系统信息 | 隧道配置 | 隧道通信状态 | 隧道协商状态

隧道通信状态

序号	本地子网	对方子网	发送成功包数	发送失败包数	发送成功字节数
1	192.168.20.0/24	192.168.10.0/24	4	0	240

图 4-30 VPN 隧道的通信情况

【注意事项】

- 实验环境地址可以随意定义，但请不要使用 1.1.1.0 这个网段的 IP，因为某些功能实现的需要，系统内部已占用该网段的部分 IP。
- 该实验中，VPN 网关的防火墙规则为全部开放。但在实际的网络环境中，如果 VPN 网关直接连接 Internet 网络，则一定需要启用防火墙规则。
- 本实验中在两个 VPN 网关上都使用了虚子网技术对原子网进行了转换，实际中只需要在一端使用虚子网技术即可避免地址重叠。

4.2 远程访问 IPSec VPN 准入控制

【实验名称】

远程访问 IPSec VPN 准入控制。

【实验目的】

学习配置远程访问(Remote Access)IPSec VPN 隧道，并且对远程接入的 VPN 用户进行准入控制。

【背景描述】

公司中某员工正在外地出差，但需要访问公司内网中的服务器资源，而这些服务器资源因安全性考虑并不直接在公网上开放，因此该员工必须通过先和公司建立 VPN 隧道，在获得访问内部资源的权力后方可允许其访问。因此出差员工通过 VPN 接入到公司内部网络，公司服务器需要对其进行一些安全检查，检查通过后方可访问，保证内部网络的安全性。

【需求分析】

需求：解决出差员工和公司之间通过 Internet 进行数据传输的安全问题，且需要进行有条件的远程接入。

分析：IPSec VPN 技术通过隧道技术、加解密技术、密钥管理技术、认证技术等有效地保证了数据在 Internet 中传输的安全性，是目前最安全、使用最广泛的 VPN 技术。可以通过建立远程访问的 IPSec VPN 加密隧道，实现出差员工和公司之间安全的数据传输。在远程用户接入到网络之前，为了保证接入到内部网络的用户不会对内部网络产生威胁，需要对接入用户的身份、系统状态等进行检查。

【实验拓扑】

如图 4-31 所示网络拓扑，是某公司员工正在外地出差，需要访问公司内网中的服务器资源。由于通过 Internet 数据传输的安全问题，公司服务器资源因安全性考虑不直接在公网上开放。外地出差员工需要远程访问总公司内网中的各种网络资源，在 Internet 上传输公司私有数据，公司希望建立 IPSec VPN 加密隧道。

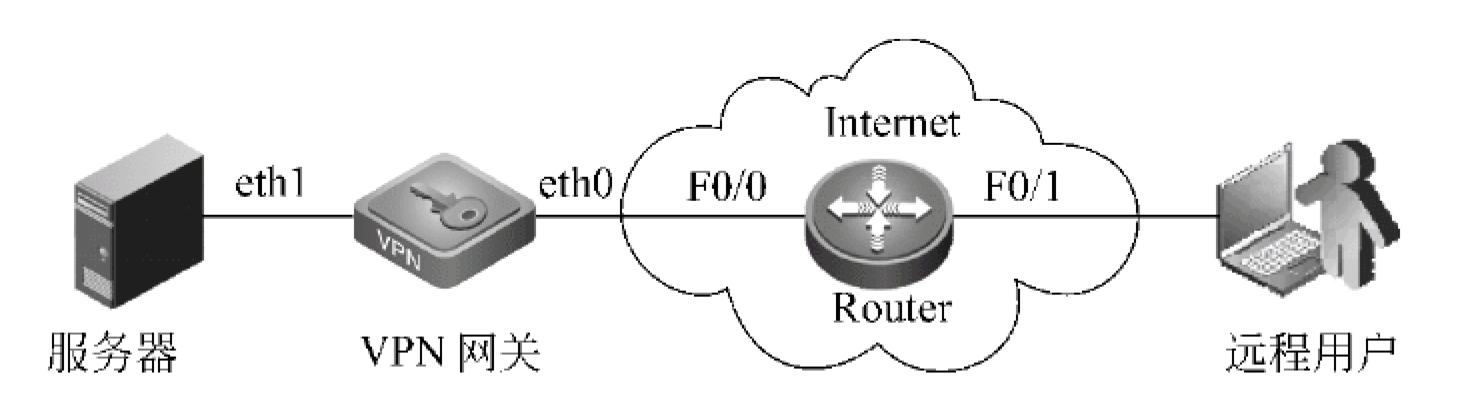


图 4-31　远程访问 IPSec VPN 准入控制网络拓扑

该员工必须通过先和公司建立 VPN 隧道，获得访问内部资源的权力，内网服务器需要对其进行一些安全检查，保证访问内部网络的安全性，才能获得访问内部资源权力，然后实现和总公司之间数据传输的安全。

【实验设备】

RG-WALL VPN 网关：1 台；RG-SRA 安全远程接入系统软件：1 套；路由器：1 台；PC：2 台（1 台作为公司内部服务器，1 台作为远程接入用户并安装 SRA 软件）。

【实验原理】

IPSec 的主要作用是为 IP 数据通信提供安全服务。IPSec 不是一个单独协议，它是一套完整的体系框架，包括 AH、ESP 和 IKE 三个协议。IPSec 使用了多种加密算法、散列算法、密钥交换方法等为 IP 数据流提供安全性，它可以提供数据的机密性、数据的完整性、数据源认证和反重放等安全服务。

使用 IPSec 可以构建两种不同接入方式的 VPN，即远程访问 VPN 安全和站点到站点 VPN 安全，本实验中使用 IPSec 来构建远程访问 VPN。

远程用户 PC 与公司 VPN 网关通过 IKE 协议，自动协商建立起远程访问 IPSec VPN 加密隧道，使得远程用户 PC 能安全地访问到 VPN 网关所保护的内部服务器。

远程用户 PC 在和 VPN 网关建立 VPN 隧道前，需要先获得 VPN 网关的身份验证许可。该实验所采用的用户身份验证为口令方式。

远程用户 PC 在通过 VPN 网关的身份验证后，VPN 网关会自动将 VPN 隧道建立（即 IKE 协商）所需要的配置下发给远程用户 PC，然后远程用户 PC 与 VPN 网关之间自动开始 IKE 协商，协商成功后 VPN 隧道即建立成功。整个过程系统自动完成，无需人为干预，是免配置的典型方式。

为了保证接入用户和其系统状态不会对内部网络产生威胁，可以在 VPN 网关侧配置接入控制功能，这样只有远程用户符合一系列的接入规则后，才允许与 VPN 网关成功建立隧道，访问内部资源。

【实验步骤】

第一步：准备好 PC 和服务器。

在实验拓扑上模拟远程用户 PC 上安装 SRA 远程接入软件，安装完成后可能需要重新启动 PC 方可生效。

在实验拓扑上模拟服务器 PC 上安装 VPN 管理软件。

具体的安装过程不在这里进行详述。

第二步：搭建拓扑，配置 IP 地址。

按照如图 4-31 所示拓扑图，搭建实验拓扑，并根据如表 4-2 所示编址方案，配置各设备的 IP 地址。

表 4-2 设备 IP 地址

设　　备	接　　口	地　　址
VPN 网关	eth1 接口地址	192.168.2.1
	eth0 接口地址	10.1.1.1
PC	PC 的 IP 地址	10.1.2.2
	PC 网关地址	10.1.2.1
服务器	服务器的 IP 地址	192.168.2.2
	服务器网关地址	192.168.2.1
Router	F0/0 地址	10.1.1.2
	F0/1 地址	10.1.2.2

说明：PC 及 Router 地址的配置方式不再详述。

(1) 通过模拟服务器的超级终端，在命令行状态下配置 VPN 网关的 eth1 口地址，操作如图 4-32 所示(注意：VPN 网关出厂时 eth1 口默认地址为 192.168.1.1/24)。

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.2.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# _
```

图 4-32 配置 VPN 网关 eth1 口地址

(2) 通过服务器上 VPN 管理软件登录 VPN 网关，然后直接双击“eht0 接口”图标，打开对话框，配置 eth0 口地址，操作如图 4-33 所示。

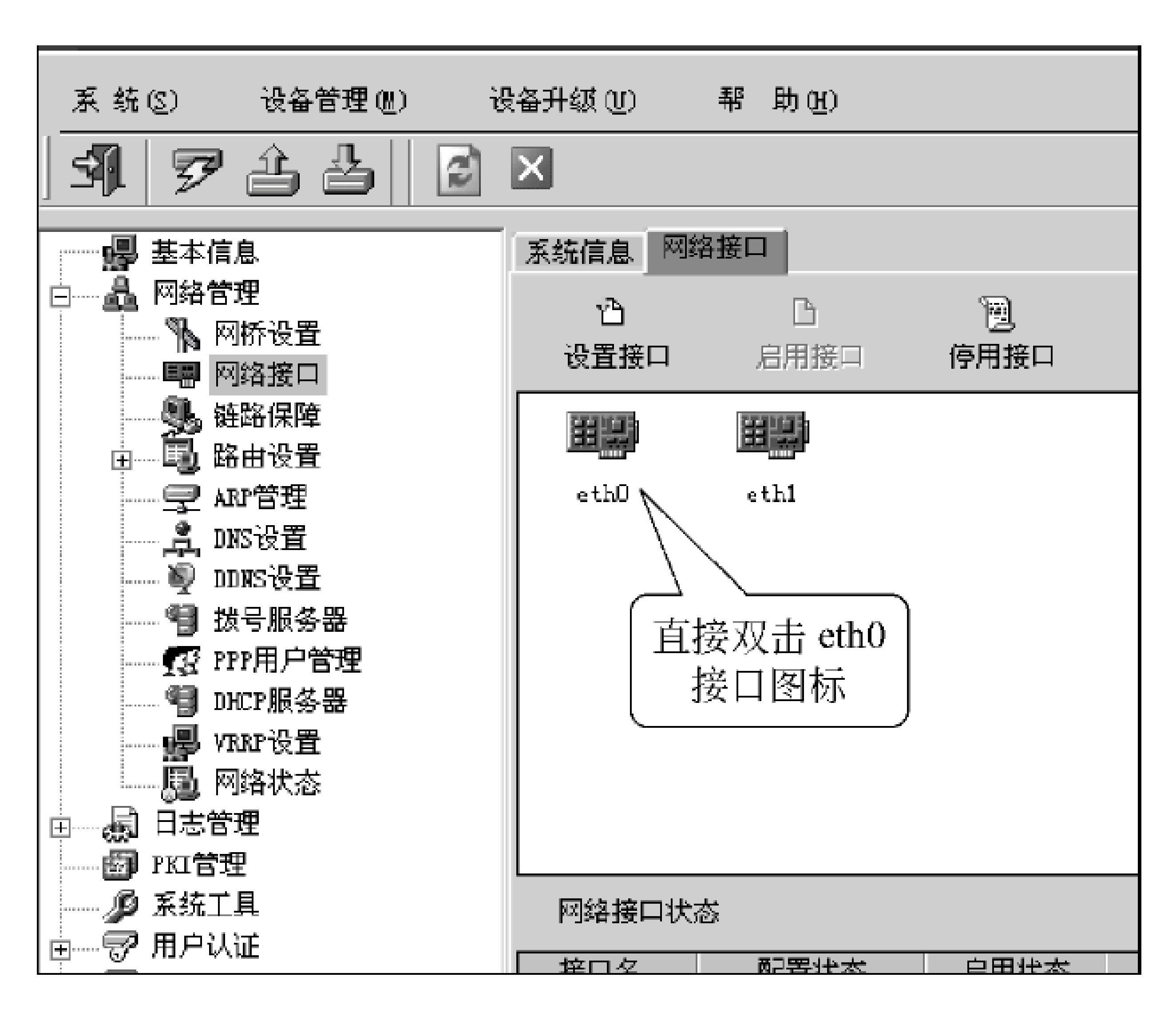


图 4-33　配置 VPN 网关 eth0 口地址(1)

按照提示的要求设置 eth0 接口地址，如图 4-34 所示。

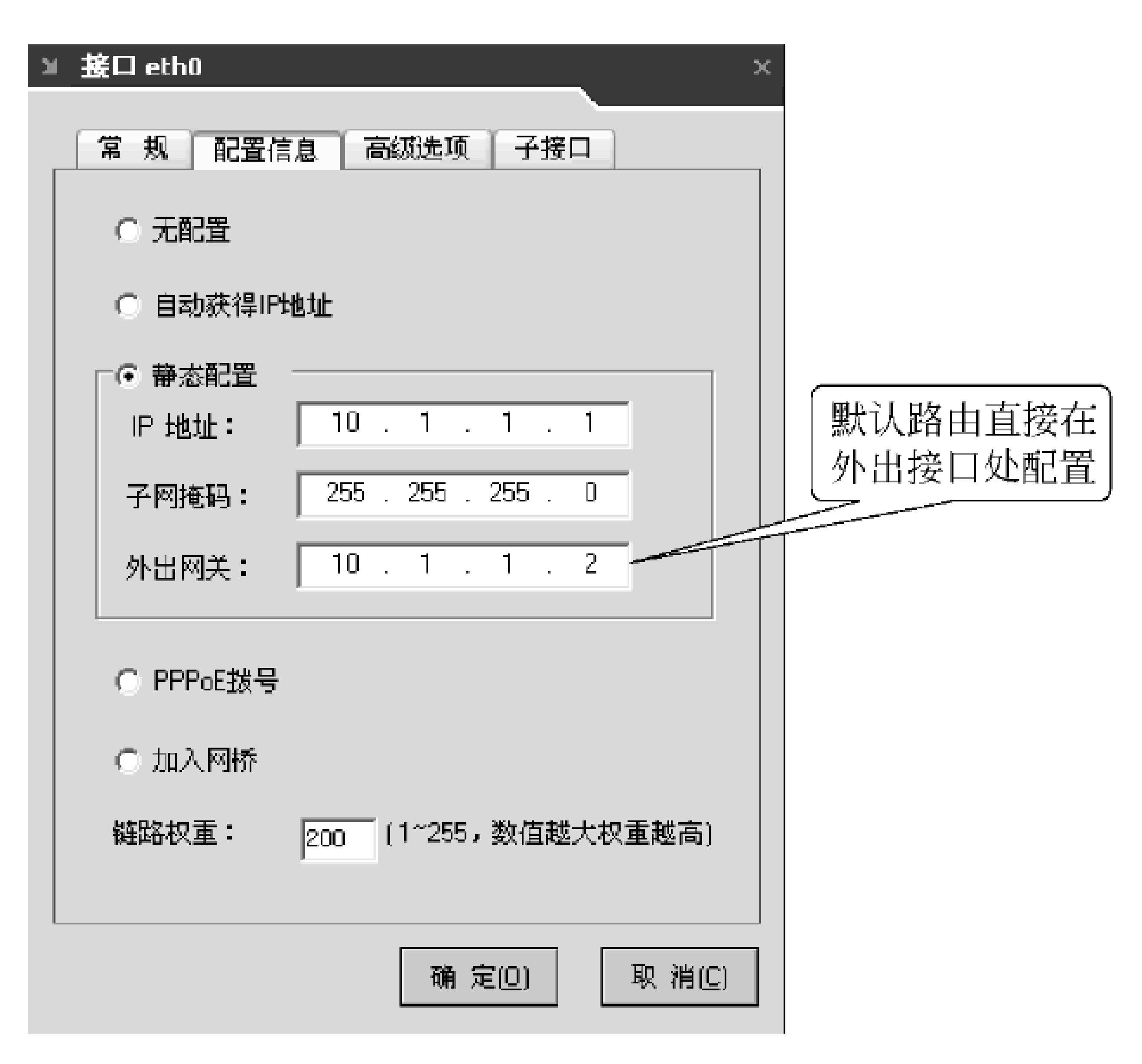


图 4-34　配置 VPN 网关 eth0 口地址(2)

第三步：配置 IPSec VPN 隧道。

(1) 进入模拟远程移动用户 VPN 隧道配置的界面。

登录 VPN 网关的管理界面，打开“虚拟专用网”中“远程用户管理”项，进入“远程用户管理”界面，如图 4-35 所示。

(2) 配置“允许访问子网”。

在图 4-35“远程用户管理”界面上，选择“允许访问子网”图标，打开配置“允许访问子网”信息，配置信息如图 4-36 所示。

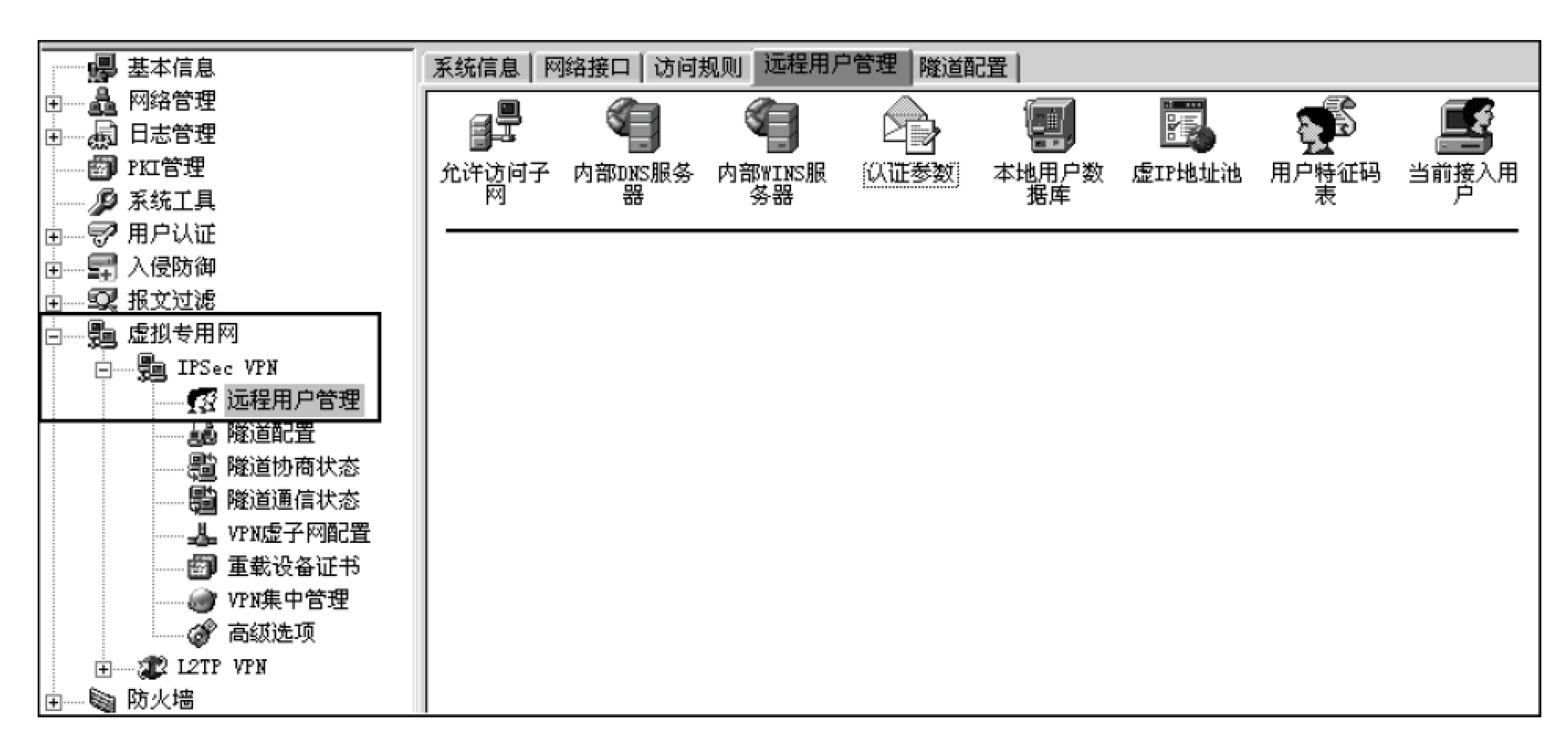


图 4-35　远程移动用户 VPN 隧道配置

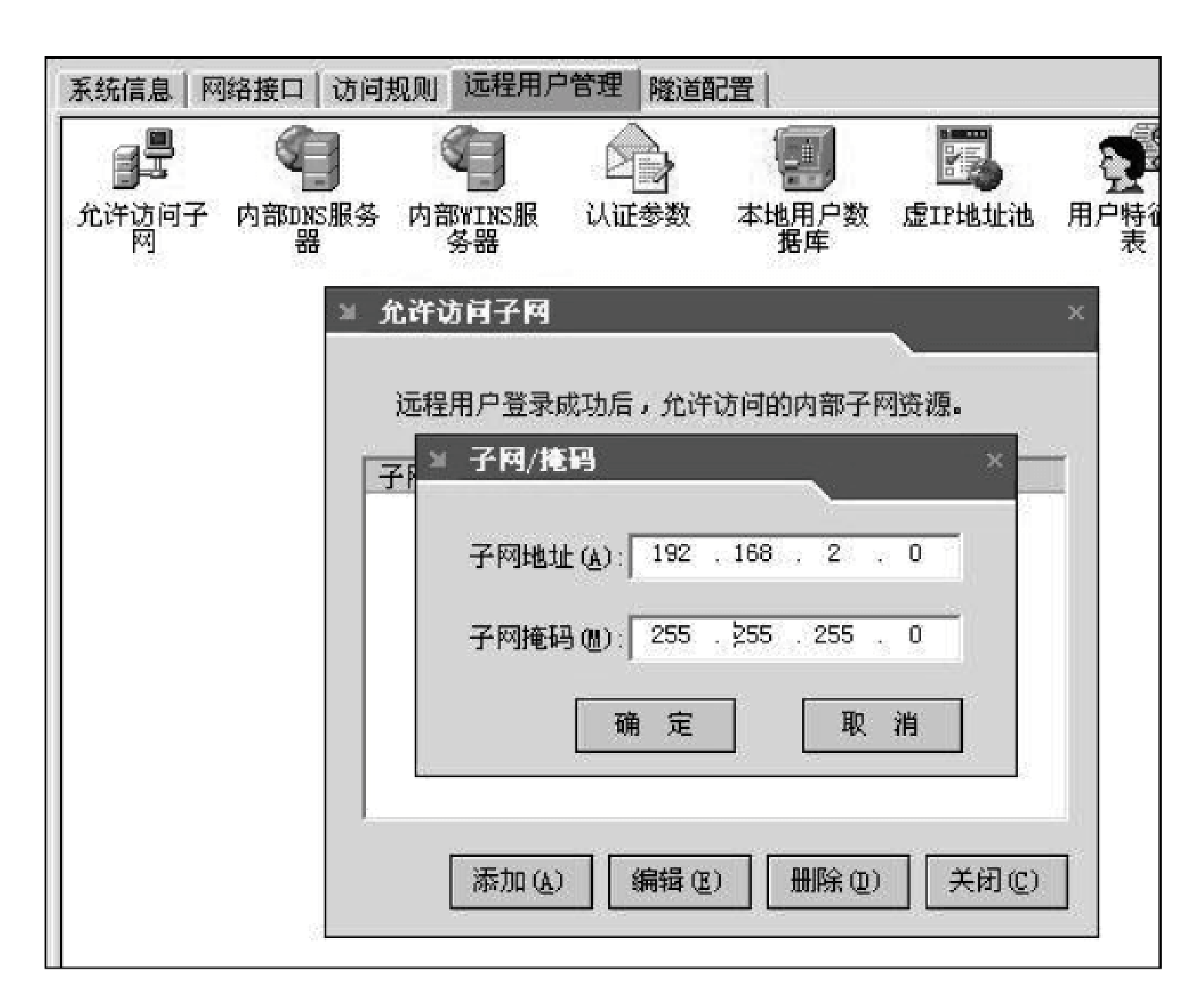


图 4-36　配置“允许访问子网”信息

(3) 配置“本地用户数据库”。

在“远程用户管理”界面上，打开配置“本地用户数据库”图标，配置信息如图 4-37 所示。



图 4-37　配置“本地用户数据库”信息

在打开的“本地用户数据库”配置界面上，单击“添加用户”按钮，为设备添加远程访问

的用户信息，包括用户名、口令和用户权限等，如图 4-38 所示，其中口令自定义。

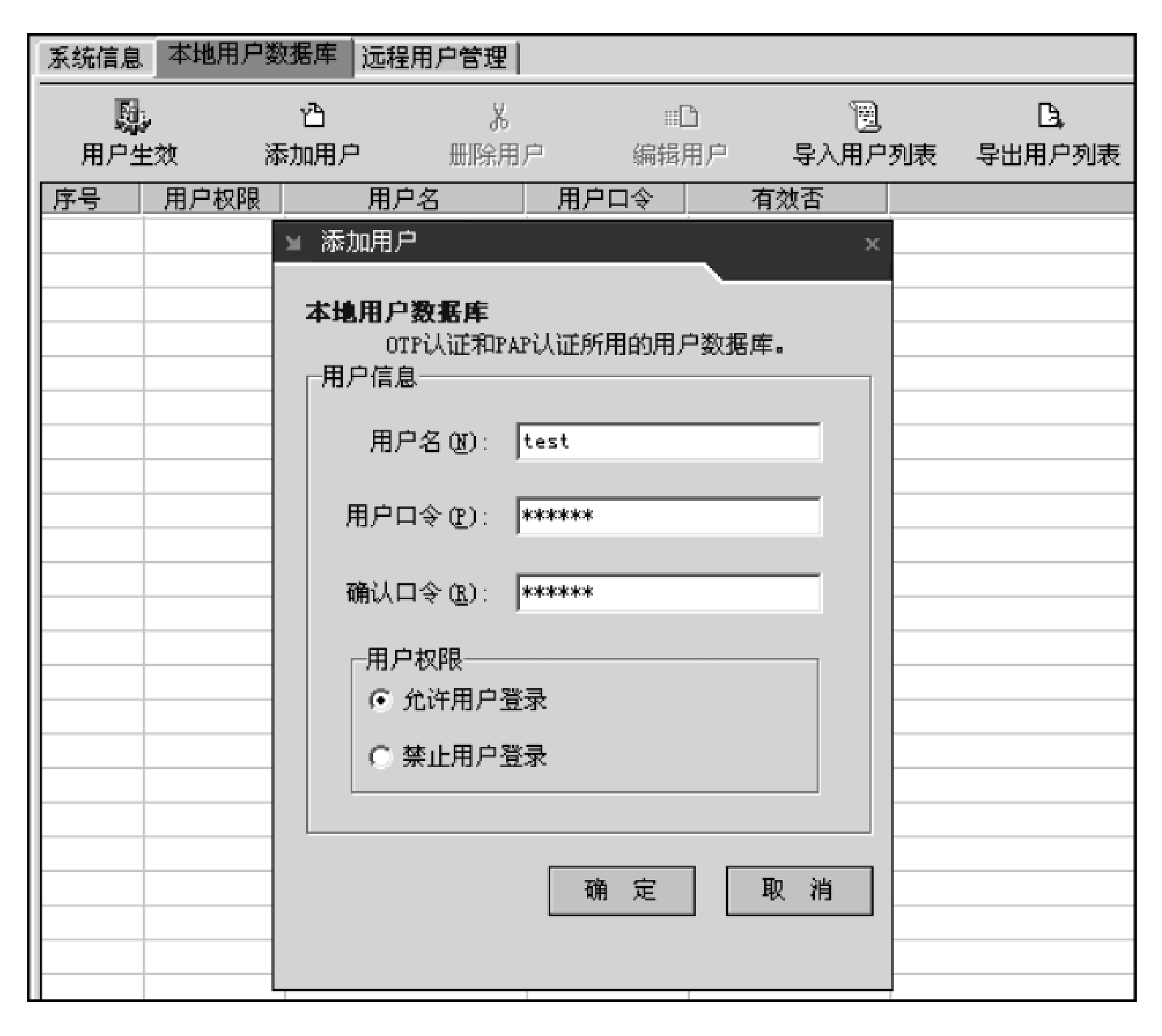


图 4-38　添加远程访问用户信息

在打开的“本地用户数据库”配置信息界面上，单击“用户生效”按钮，让配置的用户信息生效（注意：添加完用户后一定要单击“用户生效”按钮，否则新添加的用户依然不可使用），如图 4-39、图 4-40 所示。



图 4-39　让配置的用户信息生效(1)



图 4-40　让配置的用户信息生效(2)

(4) 配置“虚 IP 地址池”。

在打开的“远程用户管理”界面上选择配置“虚 IP 地址池”项，如图 4-41 所示。

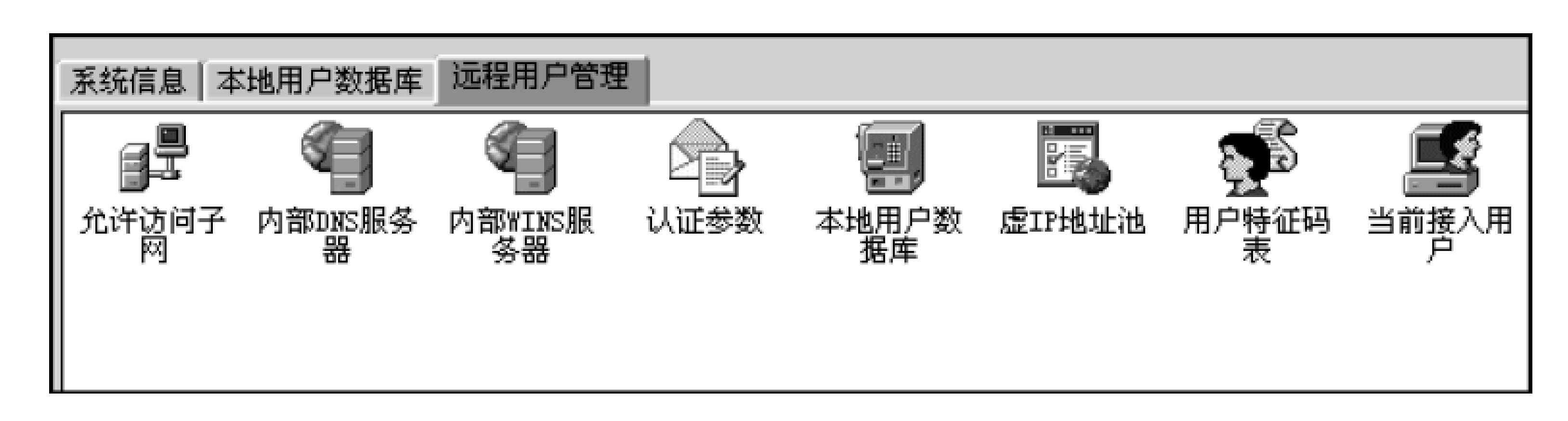


图 4-41 配置“虚 IP 地址池”信息(1)

在打开的“虚 IP 地址池”管理界面上分别选择“添加”、“删除”、“编辑”图标，配置“子网地址、连续地址”信息，如图 4-42 所示。

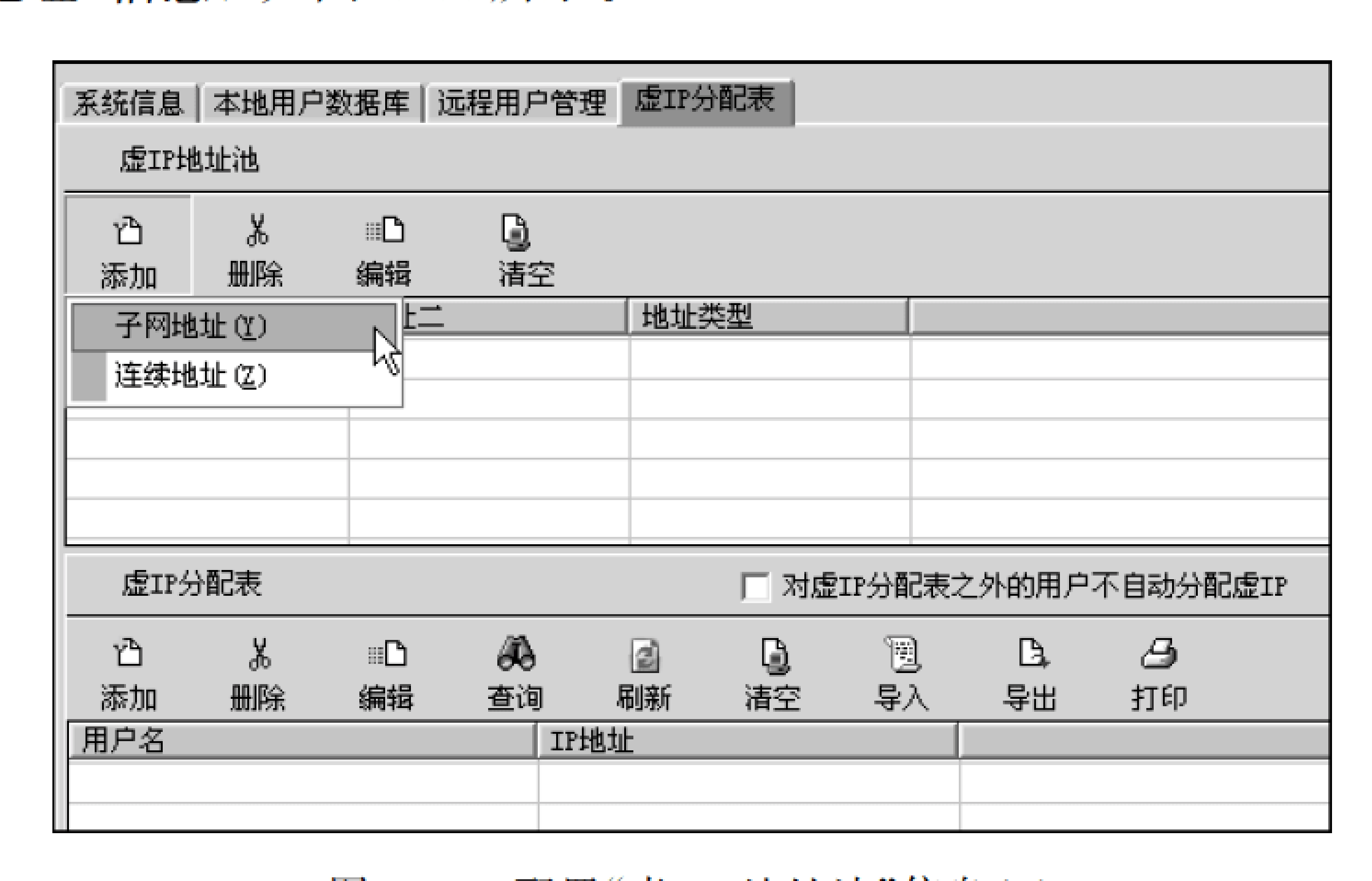


图 4-42 配置“虚 IP 地址池”信息(2)

注意：分配 PC 的虚拟 IP 地址，既可以是定义一个地址池，由 VPN 网关自动分配，也可以是管理员一个 IP 对应一个用户的分配。本实验选择地址池方式，由系统自动分配，并且选择定义“子网地址”的地址池。

虚 IP 是网络管理员分配给远程移动用户的 IP，表示只有拥有该 IP 的 PC 才能获得局域网内部的访问权限。因此，管理员设置的虚 IP 一定不要与远程 PC 的 IP，以及局域网内部的 IP 互相冲突，否则远程 PC 在和 VPN 网关建立隧道后，因地址冲突的问题，也无法访问局域网内部的服务器。本实验中虚 IP 地址池选择定义一个完全没有使用的网段。

如图 4-43 所示，在打开“虚 IP 地址池”管理界面上，选择“添加”图标，配置如图所示的子网地址信息。

如图 4-44 所示，为添加成功的虚子网地址信息。

(5) 配置“用户特征码表”。

在打开图 4-41 所示的“远程用户管理”界面上选择“用户特征码表”图标，配置“用户特征码表”信息，如图 4-45 所示。



图 4-43　配置添加子网地址信息(1)

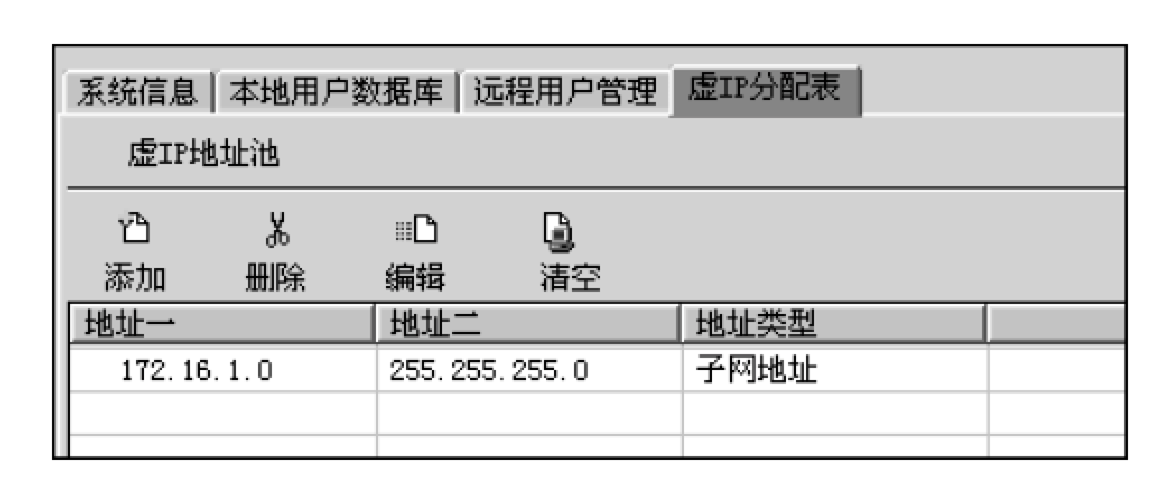


图 4-44　配置添加子网地址信息(2)



图 4-45　配置"用户特征码表"信息

打开"用户特征码表"对话框后，选择"允许接入"策略，分配接入用户的接入权限，如图 4-46 所示。



图 4-46　配置用户接入策略

配置说明："用户特征码表"是为需要将远程 PC 的硬件和分配给用户的身份信息绑定的需求而设计的。选择了"允许接入并自动绑定"功能，则 VPN 网关会将远程用户的 PC 硬件特征码与该用户的身份认证信息相互绑定，绑定后该用户将无法用自己的身份信息再在其他 PC 设备上建立 VPN 隧道。

该实验中既可以选择"允许接入"，也可以选择"允许接入并自动绑定"。系统默认配置是"禁止接入"。如图 4-46 所示选择的是"允许接入"，这表示该用户的身份信息不会和其使用的 PC 硬件绑定。此次实验，"远程用户管理"界面的其他配置项，例如，"内部 DNS 服务器"、"内部 WINS 服务器"、"认证参数"，用户可以根据实际需要选择设置。但该实验因为不涉及这些应用，故不需要进行设置。

第四步：配置远程接入客户端。

（1）第一次运行 RG-SRA 程序后，如图 4-47 所示。



图 4-47 运行 RG-SRA 程序

（2）建立一个与 VPN 网关的隧道连接。

在运行 RG-SRA 程序主界面上，单击"新建连接"按钮，建立一个与 VPN 网关的隧道连接，如图 4-48 所示。



图 4-48 新建 VPN 网关的隧道连接

在新建 VPN 网关的“添加新连接”对话框上，填写新建 VPN 网关的隧道连接的基本信息：连接标示、服务器地址、认证方式等，如图 4-49 所示。

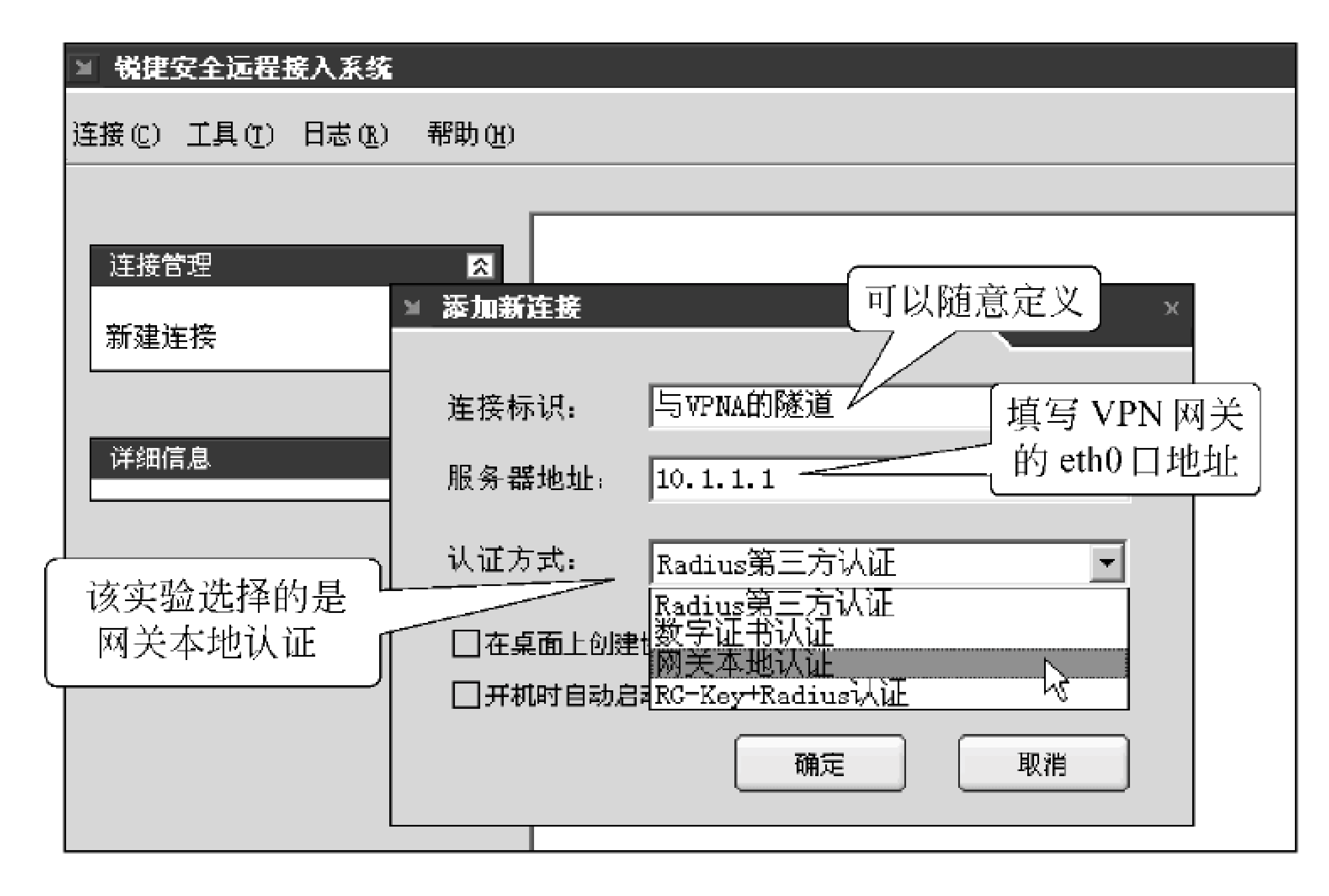


图 4-49　配置新建隧道连接的基本信息(1)

如图 4-50 所示是配置成功“新建 VPN 网关的隧道连接”基本信息。

添加新连接

连接标识：与VPNA的隧道

服务器地址：10.1.1.1

认证方式：网关本地认证

☐在桌面上创建快捷方式

☐开机时自动启动本连接

确定　取消

图 4-50　配置新建隧道连接的基本信息(2)

单击“确定”按钮后，显示建立完成的一个与 VPN 网关 A 的隧道连接标识号，如图 4-51 所示。



图 4-51　建立完成 VPN 网关的隧道连接

(3) 运行该隧道连接,建立 VPN 隧道。

在运行 RG-SRA 程序主界面上,单击“连接管理”按钮,选择新建立“与 VPN A 隧道”连接,右击打开快捷菜单,选择“启动连接”命令,启动新建的隧道连接,如图 4-52 所示。

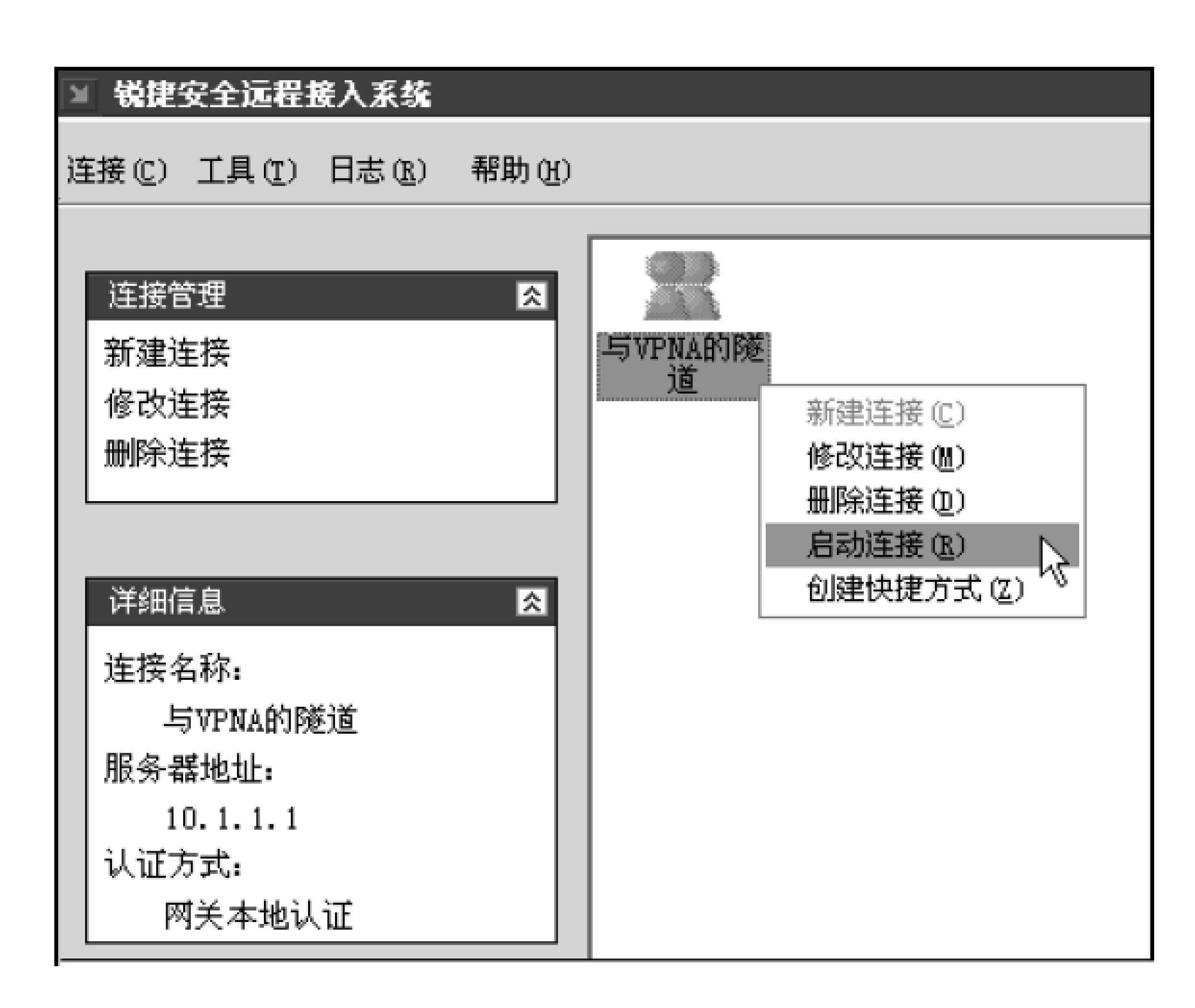


图 4-52 启动新建的隧道连接

通过“启动连接”命令,启动新建的隧道连接后,打开如图 4-53 所示 VPN 连接对话框,输入身份认证所必需的账号,即在 VPN 网关上添加的用户信息。



图 4-53 登录 VPN 远程安全接入系统

输入身份认证信息后,单击“连接”按钮后,系统自动进行身份认证,并且开始 IKE 协商,如图 4-54 所示。

系统自动进行身份认证后,与远程隧道连接建立成功,SRA 程序会自动缩小图标显示在屏幕的右下角,如图 4-55 所示。

选择 SRA 程序运行图标,右击打开快捷菜单,在菜单中选择“详细配置”,可以查看到隧道信息,如图 4-56 所示。

如图 4-57 所示信息为查看到隧道信息,显示“可访问”表示隧道已建立成功,如果是“不可访问”则表示隧道没有建立成功。“资源信息”中显示的“虚拟 IP 地址”信息,表示该 IP 为 VPN 网关从虚地址池中自动分配给该 PC 的虚 IP。



图 4-54　系统自动进行身份认证



图 4-55　SRA 程序运行成功缩小图标



图 4-56　查看到隧道信息

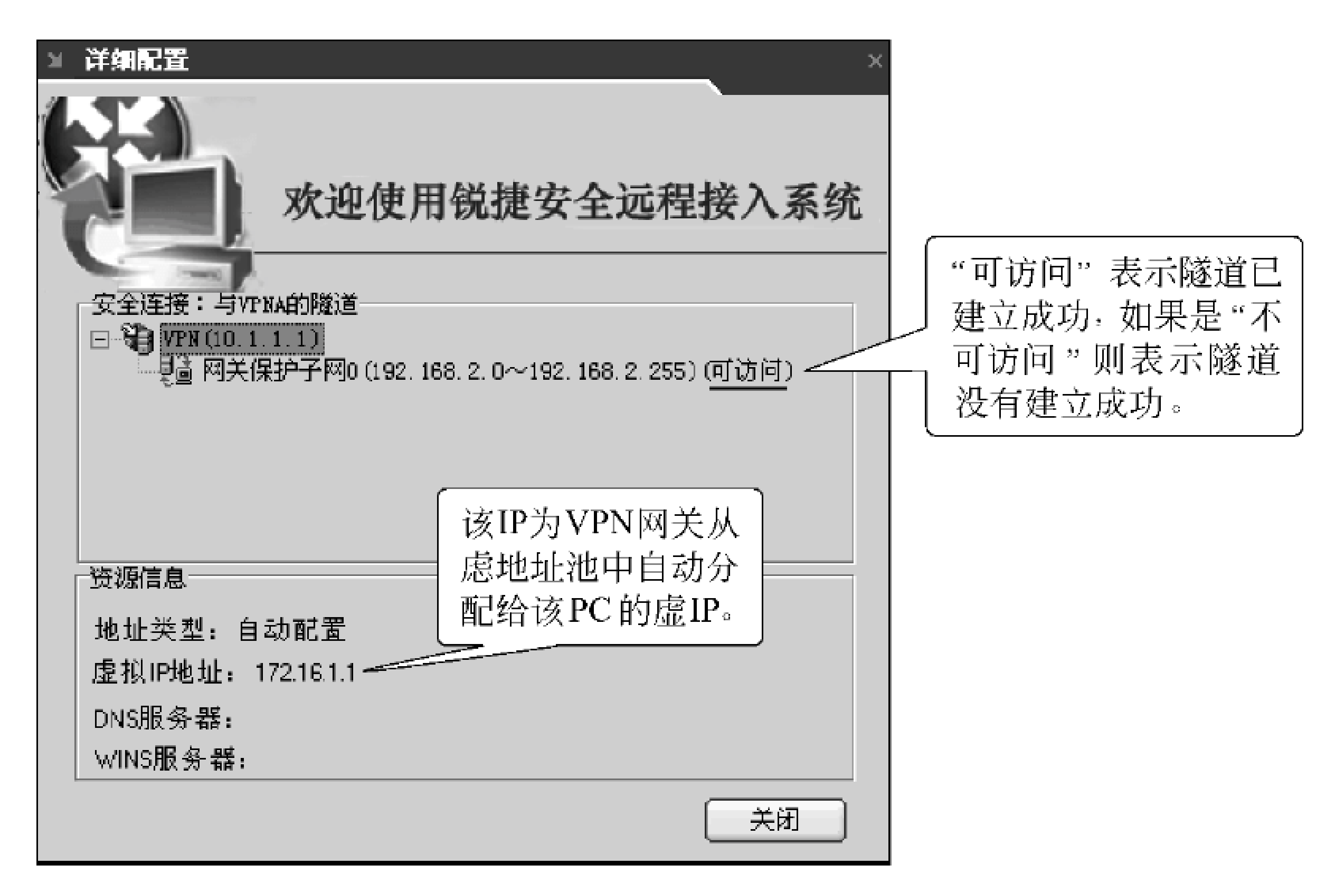


图 4-57　显示隧道配置信息内容

第五步：验证测试。

在 VPN 网关的管理界面也可看到已经建立成功的隧道信息。如图 4-58 所示信息，

在 VPN 网关的管理界面,可看到已经建立成功的隧道信息,双击“隧道协商状态”可以查看隧道协商信息。

隧道启动后,可以在“隧道协商状态”栏下看到隧道的协商状态,“隧道状态”显示“第二阶段协商成功”。VPN 隧道的通信情况可以在“隧道协商状态”中查看到,如图 4-59 所示。

图 4-58 查看隧道协商信息(1)

第六步:进行隧道通信。

在模拟远程用户 PC 上去访问服务器提供的服务可以成功,或者在 PC 上 ping 服务器的 IP 地址可以 ping 通(没有 VPN 隧道前 ping 会是失败的)。如图 4-60 所示,在 VPN 网关的管理界面选择“隧道通信状态”可以查看隧道通信信息。

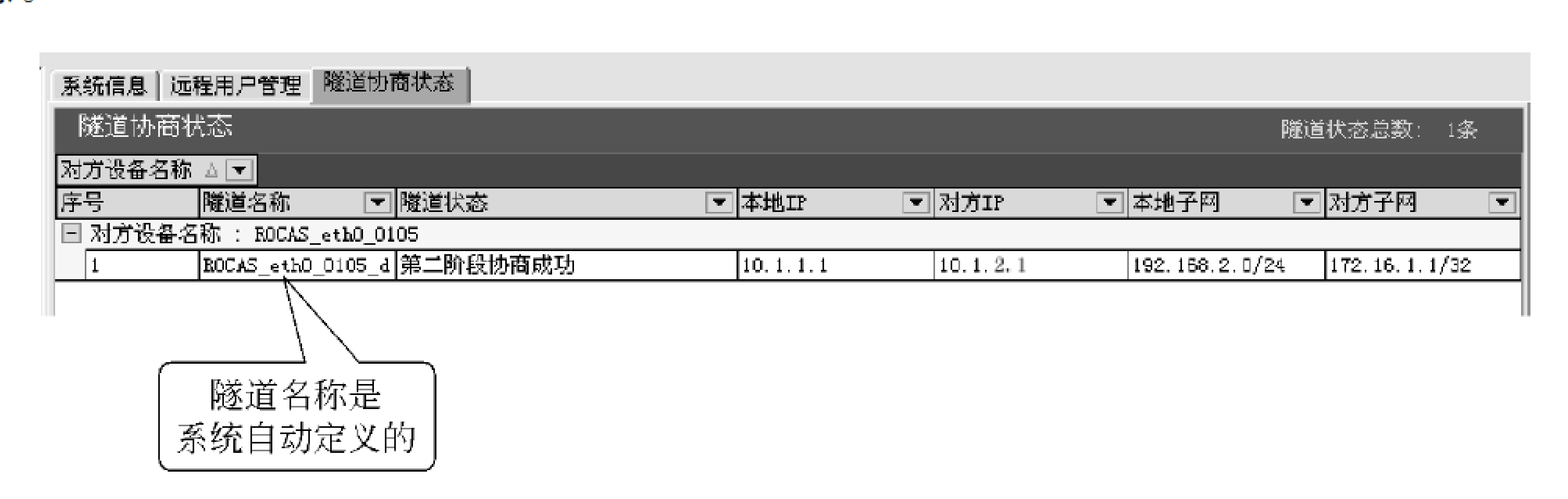


图 4-59 查看隧道协商信息(2)

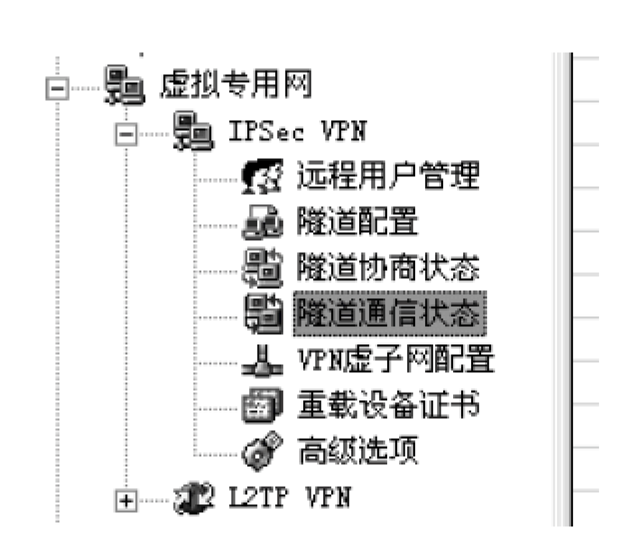


图 4-60 查看隧道通信信息(1)

隧道启动后,可以在“隧道通信状态”栏下看到隧道的通信状态,“隧道状态”显示“第二阶段协商成功”。VPN 隧道的通信情况可以在“隧道通信状态”中查看到,如图 4-61 所示。

第七步:配置客户端准入控制。

在 VPN 管理界面中,选择“虚拟专用网”→“远程用户管理”项,如图 4-62 所示。

序号	类型	本地子网	对方子网	发送成功包数	发送失败包数	发送成功字节数
1	IKE	192.168.2.0/24	172.16.1.1/32	14	0	840

图 4-61 查看隧道通信信息(2)

在 VPN 管理界面中,选择“虚拟专用网”对应的“远程用户管理”功能界面,在对话框中选择“接入控制规则表”图标,如图 4-63 所示。

(1) 配置访问控制。

在“远程用户管理”功能界面上，双击“接入控制规则表”启动配置对话框，如图 4-64 所示。

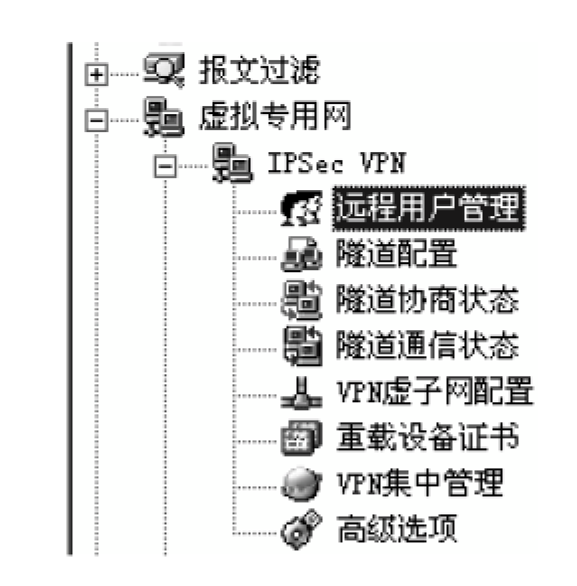


图 4-62 选择虚拟专用网远程用户管理

选择“访问控制”选项卡，单击右侧“添加”按钮，添加一条访问控制规则。其中规则名称为 TCP 控制，规则动作设置为“通过”，协议类型选择 TCP，远程地址选中单个地址并填入服务器地址 192.168.2.2，远程端口和本地端口都选择所有端口，配置信息如图 4-65 所示。

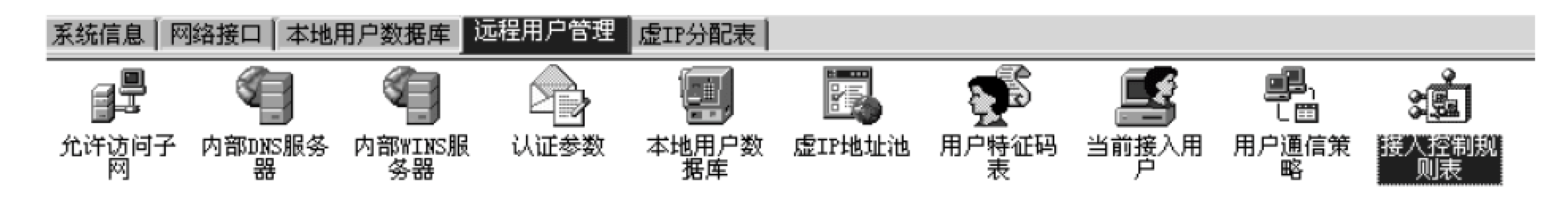


图 4-63 选择接入控制规则表



图 4-64 配置访问控制规则(1)

配置完成后，单击“确定”按钮，成功添加一条访问控制规则，如图 4-66 所示。

选择该规则，单击“确定”使配置生效。重新使用远程客户端进行连接，客户端登录成功后，在客户端 PC 上建立到达服务器的 TCP 连接(例如 FTP、Telnet)，如果连接成功，说明访问控制规则配置生效。选中刚才添加的访问控制规则，单击“编辑”，把规则动作设置为“阻断”，重新使用远程客户端进行连接。客户端登录成功后，在客户端 PC 上建立到达服务器的 TCP 连接(例如 FTP、Telnet)，连接将不成功。

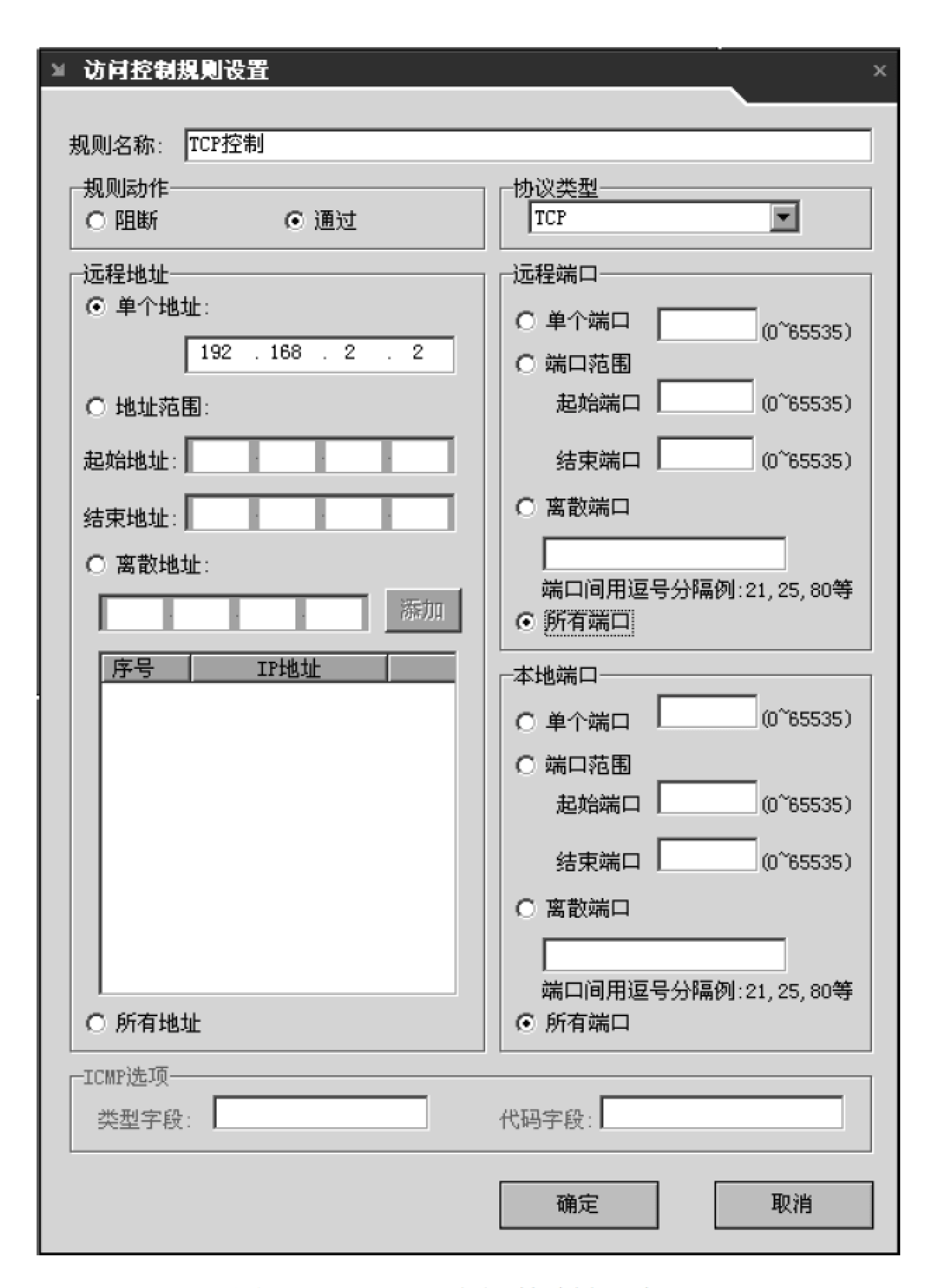


图 4-65　配置访问控制规则(2)



图 4-66　成功添加一条访问控制规则

(2) 进程检查控制实验。

在图 4-63 “远程用户管理”功能界面上，双击“接入控制规则表”项，启动配置对话框，选择“进程检查”选项卡，如图 4-67 所示。



图 4-67　启动进程检查

单击右侧“添加”按钮，弹出添加“进程检查”规则的对话框，如图 4-68 所示。

单击“浏览”按钮，选中一进程文件，如路径为 C:\WINDOWS\system32\cmd.exe，即系统命令行窗口 exe 文件，进程名称处填入容易识别的名称，如 cmd.exe，判断标识选择“允许”，如图 4-69 所示。



图 4-68　配置启动进程检查(1)



图 4-69　配置启动进程检查(2)

单击“确定”，成功添加一条进程检查规则，如图 4-70 所示。

如果客户端 PC 系统打开了命令行窗口，此时进行客户端登录，系统会提示“危险进程 cmd.exe”存在，如图 4-71 所示。

如果客户端 PC 系统没有运行命令行窗口，此时进行客户端登录，可以成功登录。

(3) 操作系统检查实验。

在图 4-67 “接入控制规则表”功能界面上，选中“操作系统检查”项，如图 4-72 所示。

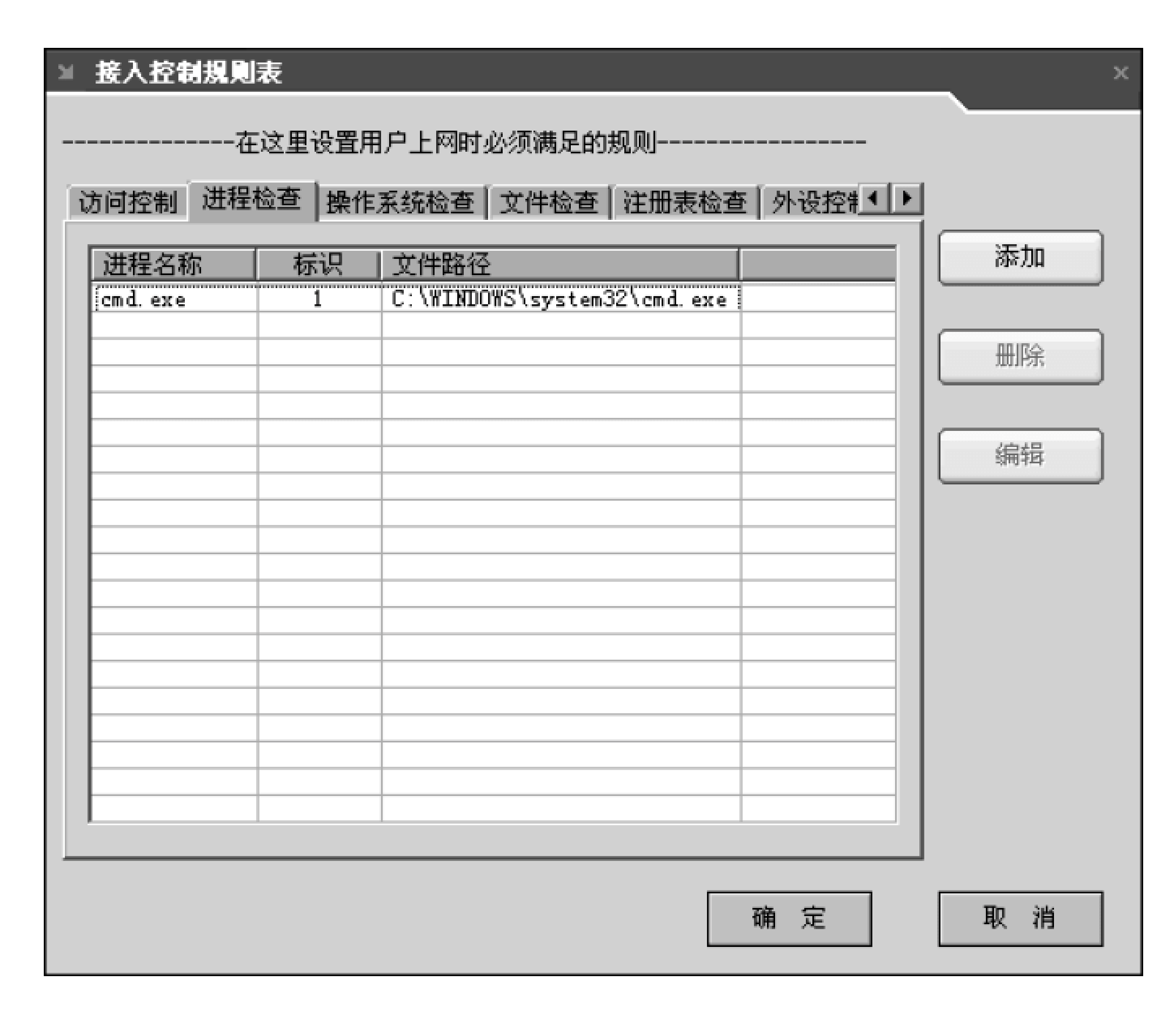


图 4-70　添加一条进程检查规则

在“接入控制规则表”功能界面上，选中“操作系统检查”项，单击“添加”按钮，添加一条“操作系统检查”规则，如图 4-73 所示。

在添加的“操作系统检查”规则中，选择 Windows XP 操作系统，按“确定”后，弹出“设置系统补丁包”对话框，系统补丁填写 SP3，如图 4-74 所示。



图 4-71　系统检查提示信息



图 4-72　选中“操作系统检查”项

单击“确定”按钮完成添加。重新使用远程客户端进行连接，因为用户 PC 系统为 Windows XP，补丁包为 SP2，所以客户端登录系统会提示“操作系统补丁版本过低，请更新”，如图 4-75 所示。

（4）注册表检查控制实验。

在图 4-67 “接入控制规则表”功能界面上，打开“注册表检查”选项卡，如图 4-76 所示。

在打开“注册表检查”对话框中，单击“添加”按钮打开注册表添加窗口，如图 4-77 所示。



图 4-73　启动操作系统检查功能

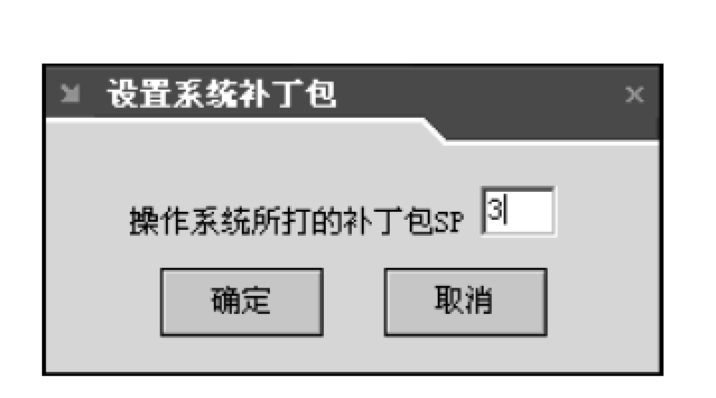


图 4-74　填写系统补丁



图 4-75　配置操作系统检查测试



图 4-76　配置注册表检查

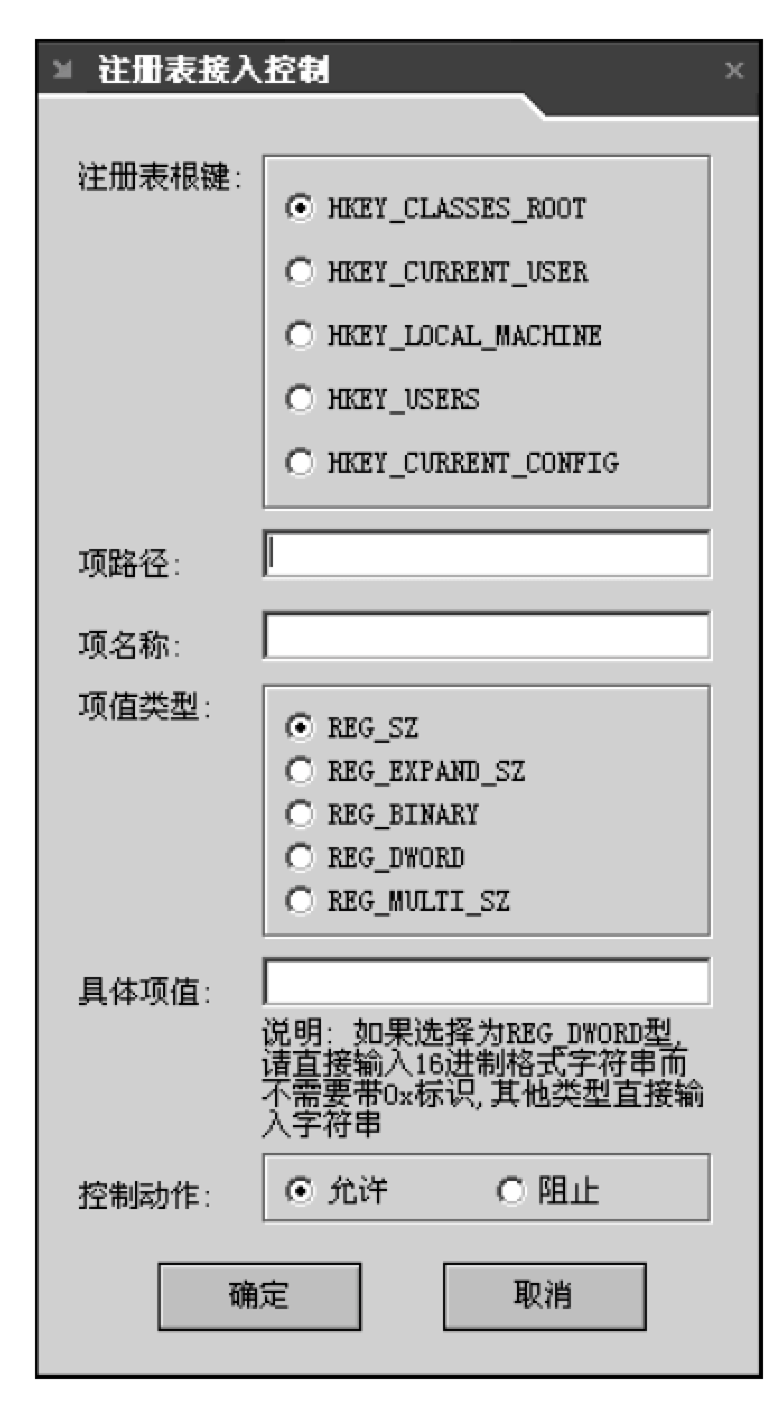


图 4-77　“添加”窗口

验证测试准备：配置结束后，回到操作系统控制面板上，使用命令打开 PC 系统的注册表，查找需要填入注册表接入控制规则的内容，如图 4-78 所示。

在图 4-78 所示中，在注册表根键 HKEY_CLASSES_ROOT 下路径为.323 项名称为 Content Type，项值类型为 REG_SZ，有一项值为 text/h323 具体项，把上述值分别填入注

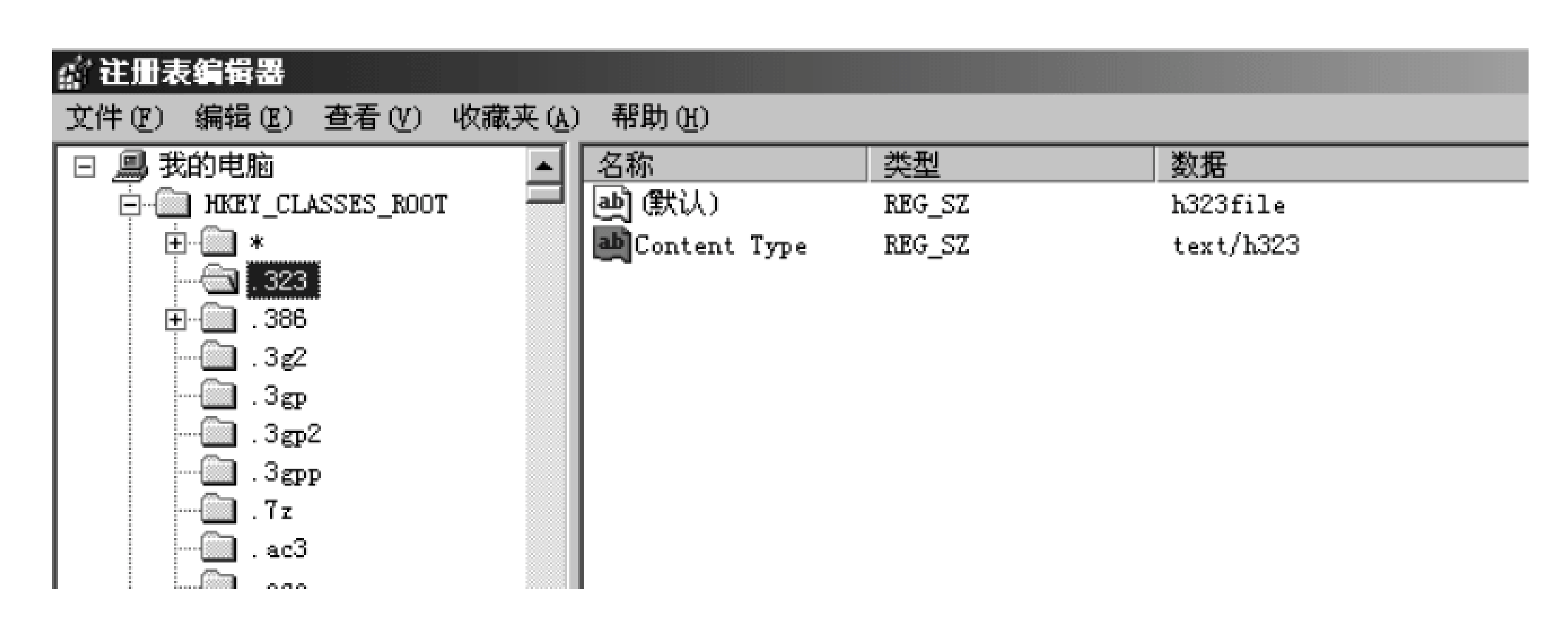


图 4-78　验证测试配置完成的注册项

册表接入控制规则中,其中规则动作设置为"允许",如图 4-79 所示。

在图 4-79 所示注册表接入控制规则项中,选择配置相关规则,单击"确定"按钮,成功添加一条注册表接入控制规则,如图 4-80 所示。

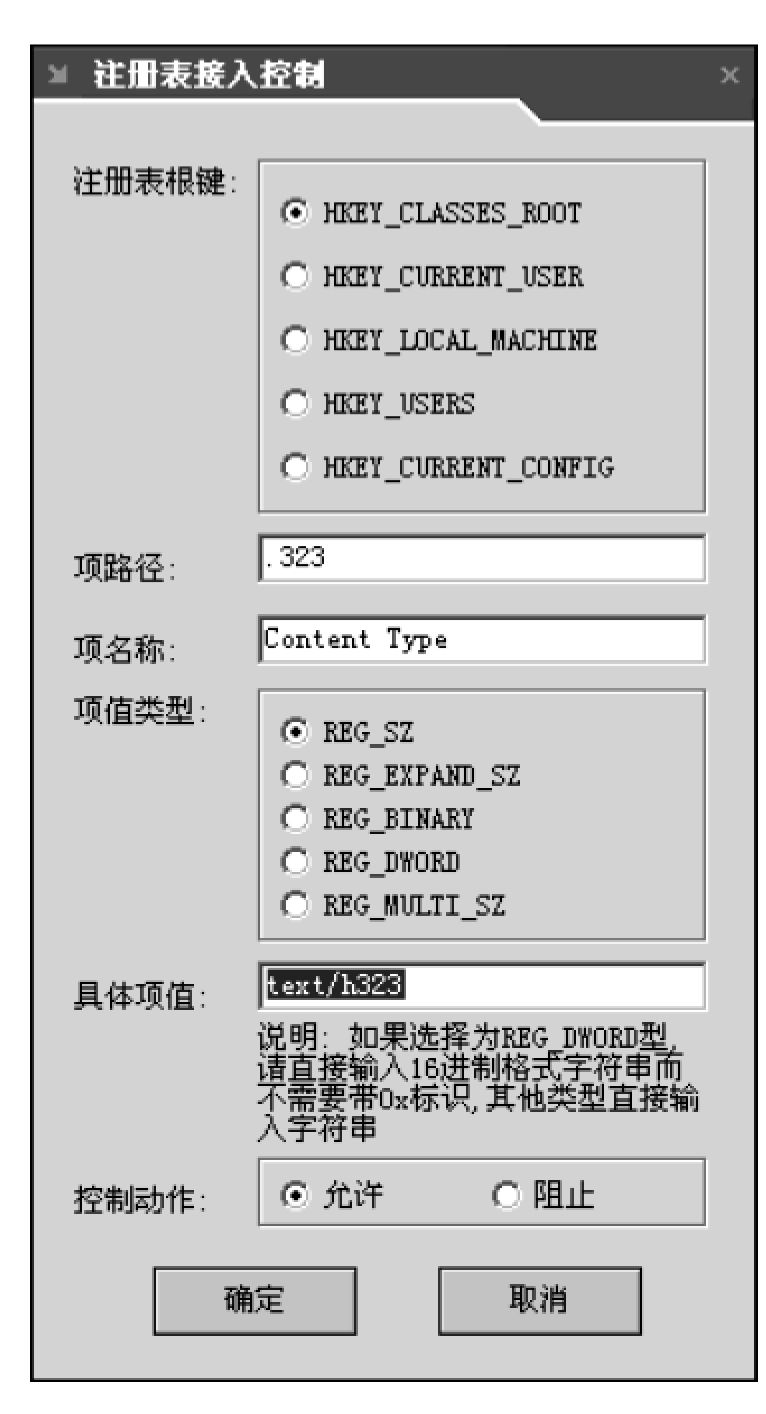


图 4-79　配置注册表接入控制规则



图 4-80　配置完成的注册表接入控制规则

单击"确定"按钮,使规则生效。重新登录远程客户端,将连接成功。

如果上述添加的规则控制动作设置为"阻止",客户端系统会提示"存在危险注册表项.323\Content Type!"从而拒绝客户端登录,如图 4-81 所示。



图 4-81　规则验证测试

(5) 外设控制实验。

在图 4-67 所示的 "接入控制规则表"功能界面上,打开"外设控制及安全检查"选项

卡，配置相关信息，如图 4-82 所示。

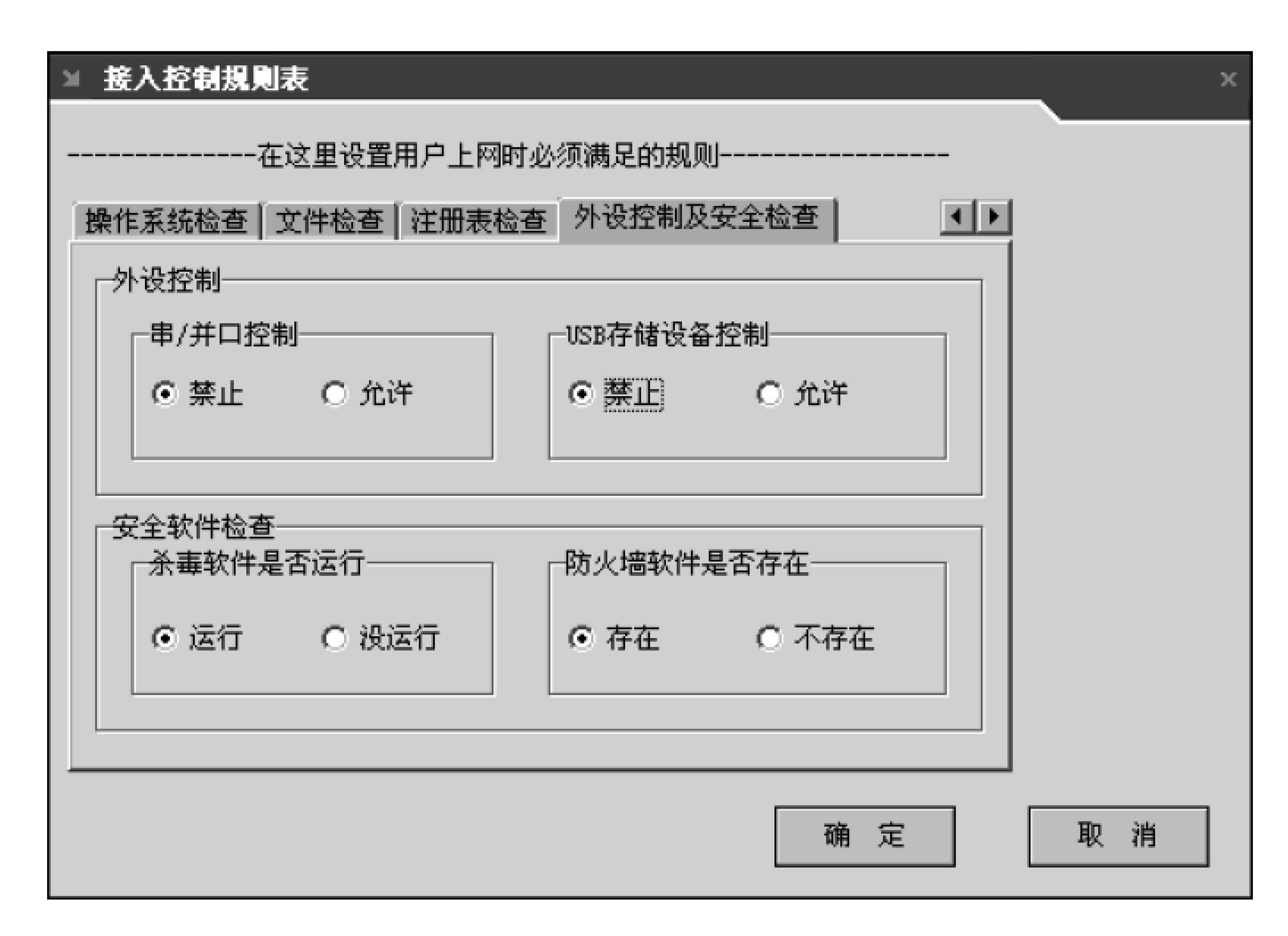


图 4-82　启动“外设控制及安全检查”项

验证测试准备：外设控制默认配置的串/并口控制为“禁止”，USB 存储设备控制为“禁止”。使用远程客户端重新登录，客户端会成功登录。查看用户 PC 的“设备管理器”，发现串/并口都被禁用，如图 4-83 所示。



图 4-83　验证测试外设控制及安全检查准备

验证测试：在用户 PC 上插入一 U 盘，双击 U 盘盘符，系统会提示“请将磁盘插入驱动器 I:”，如图 4-84 所示。

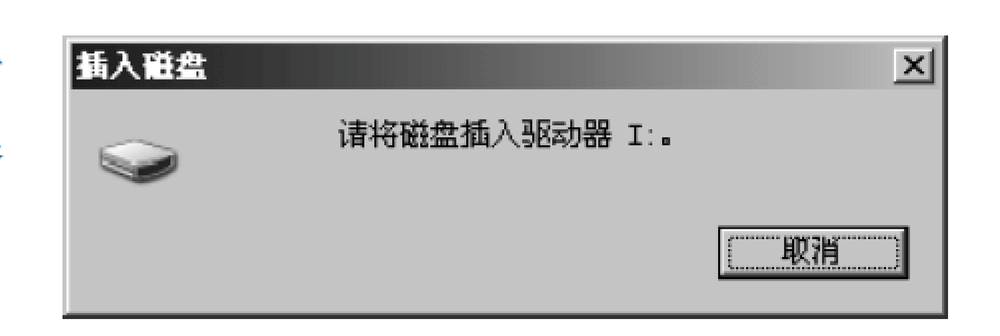


图 4-84　禁止 U 口后插入 U 盘提示信息

(6) 安全检查控制实验。

在“接入控制规则表”对话框中打开“外设控

制及安全检查"选项卡，配置如图 4-85 所示配置相关控制信息。

图 4-85　配置安全检查控制规则

安全软件检查默认配置杀毒软件是否运行栏为"运行"，防火墙软件是否存在栏为"存在"，重新使用远程客户端登录，会有如下几种可能。

- 如果客户端运行了杀毒软件也运行了防火墙，客户端会登录成功。
- 如果客户端运行了杀毒软件而没有运行防火墙，系统会提示"防火墙软件不存在"，拒绝客户端登录，如图 4-86 所示。
- 如果客户端没有运行杀毒软件，系统则会提示"杀毒软件不存在"，拒绝客户端登录。

【注意事项】

- 实验环境地址可以随意定义，但请不要使用 1.1.1.0 这个网段的 IP，因为某些功能实现的需要，VPN 系统内部已占用该网段的部分 IP。
- 该实验中，VPN 网关的防火墙规则为全部开放。但在实际的网络环境中，如果 VPN 网关直接连接 Internet 网络，则一定需要启用防火墙规则。
- RG-SRA 是 VPN 客户端软件程序，如果 PC 上已预装其他厂家的 VPN 客户端程序，请先卸载其他厂家的 VPN 客户端程序，否则 RG-SRA 可能无法正常工作。
- RG-SRA 作为安全产品，安装后会对系统的网卡、端口、协议等方面有改动，因此会和部分防火墙或者防病毒程序不兼容。推荐用户使用没有安装任何第三方防火墙、防病毒程序的机器来做实验。
- 注册表接入控制规则中，项路径和项名称前请不要加"\"，直接填写具体路径即可，否则规则无法生效，如图 4-87 所示。
- 接入控制功能中，"访问控制"选项是客户端成功接入后，对用户访问进行控制，而其他选项则是对客户端接入前做判断，如果不满足规则则拒绝接入。



图 4-86　防火墙安全配置规则

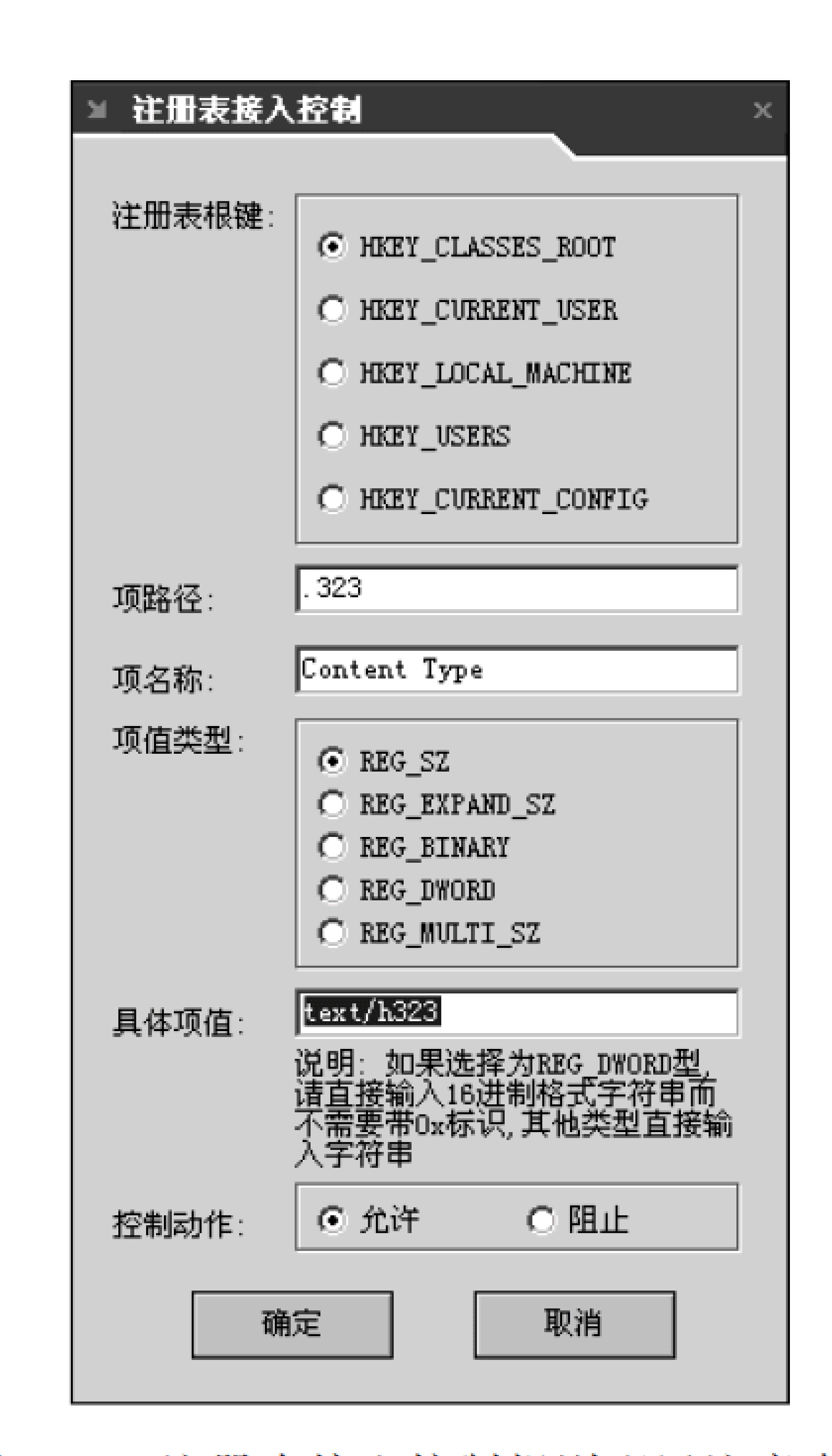


图 4-87　注册表接入控制规则配置注意事项

4.3　构建 SSL VPN

【实验名称】

构建 SSL VPN。

【实验目的】

学习配置 SSL VPN 隧道,加深对 SSL VPN 的理解。

【背景描述】

某公司为了员工出差时能随时随地和公司总部网络联络,共享公司内网中包括业务处理、资源访问、资源共享等资源。公司希望员工能够通过公网方便接入到公司网络中。由于出差在外员工可能会使用不同的电脑,甚至是在网吧中,所以公司不希望员工通过使用额外软件实现接入公司内网,这就要求为出差在外员工提供一种安全、灵活、快速、方便的远程 VPN 接入方式。

【需求分析】

需求:解决出差员工和公司之间,通过 Internet 公网进行数据传输的安全问题,保证在使用上快速、便捷、灵活的方式接入。

分析:通过使用 SSL VPN 技术,远程用户可以接入到公司内部网络,并且与公司内部的通信数据在 Internet 上传输时都是经过加密。此外,SSL VPN 的最大优势是部署灵

活、方便,无需预先为接入 PC 安装远程接入软件(例如 IPSec 客户端等),真正地实现了零配置安全接入。

【实验拓扑】

如图 4-88 所示网络拓扑,是某公司在上海设立了分公司,分公司要远程访问总公司的各种网络资源,实现分公司和总公司之间信息共享。为解决上海分公司和北京总公司之间通过 Internet 进行数据传输的安全问题,公司希望通过 SSL VPN 技术,有效保证数据在 Internet 网络传输的安全问题。

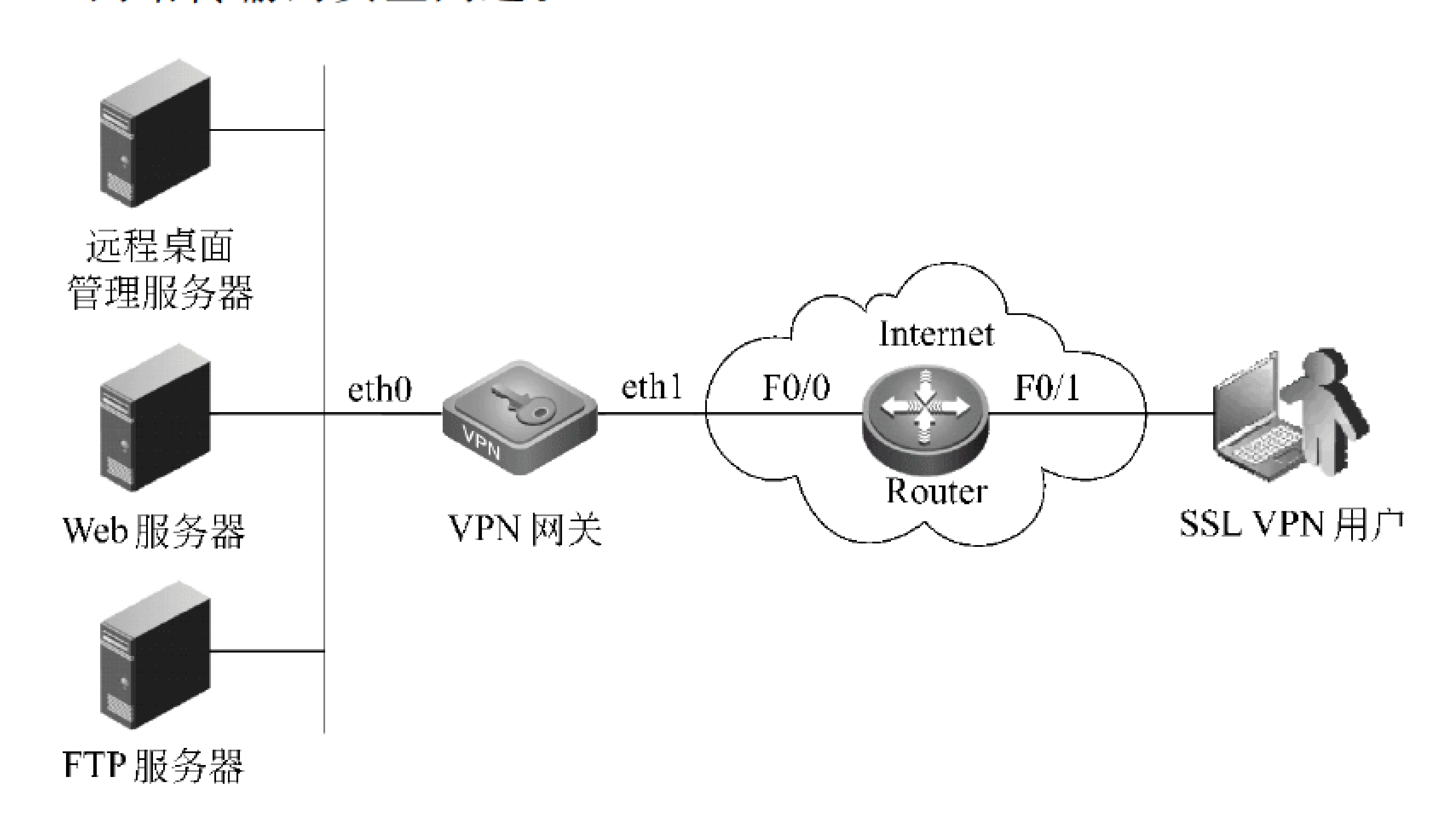


图 4-88 构建 SSL VPN 网络拓扑

出差在外员工可能会使用不同地方的电脑接入到公司网络中,公司不希望员工通过使用额外软件实现接入,希望使用 SSL VPN 技术,提供一种安全、灵活、快速、方便的远程接入方式,实现方便、安全通信。

【实验设备】

RG-WALL V1000 VPN 网关:1 台;路由器:1 台;PC:4 台。

【预备知识】

SSL VPN 工作原理

随着应用程序从客户机和服务器(C/S)结构向 Web 模式的迁移,企业必须面对一个新的挑战,就是如何在不影响最终用户使用的前提下,实现在任何地方灵活访问这些应用程序。公司管理者和销售员在外出差时携带笔记本电脑,需要实时访问公司内部信息,设立 IPSec VPN 可以保护用户远程访问,提供足够安全性,但问题是安装和维护相当麻烦。

任何在 PC 上的改变,对 VPN 而言可能都是一件很麻烦的网络改造工作。从管理员角度来讲,使用 IPSec VPN 不仅仅意味着要对客户端进行安装和调试,而且还需要调整整个网络结构。

租用 WAN 线路使用 IPSec VPN,对于不经常更改网络结构的用户来说是非常好的选择,通过 SSL VPN 技术解决远程用户访问公司敏感数据最简单最安全的解决方案。与复杂的 IPSec VPN 相比,SSL 协议通过简单易用的方法,实现信息远程连通。任何安

装浏览器的 PC 都可以使用 SSL VPN，这是因为 SSL 内嵌在浏览器中，它不需要像传统 IPSec VPN 一样必须为每一台客户机安装客户端软件。

使用 SSL VPN，人们可以通过 IP 浏览器安全访问应用程序。任何安装浏览器的机器都可以使用 SSL VPN，不需要像传统 IPSec VPN 一样，必须为每一台客户机安装客户端软件。这一点对需要使用大量机器（包括家用机、工作机和客户机等）与公司机密信息相连接的网络场景至关重要。

SSL VPN 即指采用 SSL（Security Socket Layer）协议实现远程接入一种新型 VPN 技术。SSL 协议是网景公司提出基于 Web 应用安全协议，它包括服务器认证、客户认证（可选）、SSL 链路上数据完整性和 SSL 链路上数据保密性。使用 SSL 可保证信息真实性、完整性和保密性。

目前 SSL 协议被广泛应用于各种浏览器，也可以应用于 Outlook 等使用 TCP 协议传输数据 C/S 应用。正因为 SSL 协议被内置于 IE 等浏览器中，使用 SSL 协议进行认证和数据加密可以免于安装客户端。相对于传统 IPSec VPN 而言，SSL VPN 具有部署简单，无客户端程序，维护成本低，网络适应强等特点。

SSL 协议

SSL 是 Secure Socket Layer 的缩写，即安全套接层协议。是由网景（Netscape）公司推出的一种安全通信协议，它能够对信用卡和个人信息提供较强的安全保护。SSL 协议是对计算机网络之间整个会话进行加密的协议。在 SSL 中，采用了公开密钥和私有密钥两种加密方法。SSL 协议用以保障在 Internet 上数据传输的安全，利用数据加密技术，可确保数据在网络上的传输过程中不会被截取及窃听。目前一般通用规格为 40 位加密安全标准，更高安全则已推出 128 位标准。SSL 协议已被广泛地用于 Web 浏览器与服务器之间的身份认证和加密数据传输。

SSL 协议的优势在于它与应用层协议无关，高层的应用协议如 HTTP、FTP、Telnet 等都能透明地建立于 SSL 协议之上，其在应用层协议通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作。在此之后应用层协议所传送的数据都会被加密，从而保证通信的安全性。

SSL 协议提供的安全服务有：

① 对用户和服务器合法性认证，确保数据将被发送到正确客户机和服务器上；

② 加密数据以隐藏被传送的数据，以确保数据传输过程中机密性和数据完整性，加密数据以防止数据中途被窃取；

③ 维护数据的完整性，确保数据在传输过程中不被改变。

SSL 协议的主要目的是在两个通信应用程序之间提供私密信和可靠性，SSL 协议位于 TCP/IP 协议与各种应用层协议之间，为数据通信提供安全支持。这个过程通过 3 个元素来完成。

① SSL 握手协议（SSL Handshake Protocol）：它建立在 SSL 记录协议之上，用于在实际的数据传输开始前，通信双方进行身份认证、协商加密算法、交换加密密钥等。这个协议负责协商被用于客户机和服务器之间会话的加密参数。当一个使用 SSL 协议客户机和服务器第一次开始通信时，它们在一个协议版本上达成一致，选择加密算法，选择相

互认证，并使用公钥技术来生成共享密钥；

② SSL 记录协议(SSL Record Protocol)：它建立在可靠的传输协议(如 TCP)之上，为高层协议提供数据封装、压缩、加密等基本功能的支持，这个协议用于交换应用层数据。应用程序消息被分割成可管理的数据块，通过压缩，并应用一个 MAC(消息认证代码)，然后结果被加密传输。接受方接受数据并对它解密，校验 MAC，解压缩并重新组合它，并把结果提交给应用程序协议；

③ 警告协议。这个协议用于指示在什么时候发生了错误或两个主机之间的会话在什么时候终止。

SSL 协议的工作流程。

服务器认证阶段：①客户端向服务器发送一个开始信息 Hello 包，以便开始一个新的会话连接；②服务器根据客户的信息确定是否需要生成新的主密钥，如需要则服务器响应客户的 Hello 信息，并生成主密钥所需的信息；③客户根据收到的服务器响应信息，产生一个主密钥，并用服务器的公开密钥加密后传给服务器；④服务器恢复该主密钥，并返回给客户一个用主密钥认证的信息，以此让客户认证服务器。

用户认证阶段：在此之前，服务器已经通过了客户认证，这一阶段主要完成对客户的认证。经认证的服务器发送一个提问给客户，客户则返回(数字)签名后的提问和其公开密钥，从而向服务器提供认证。

下面来看一个使用 Web 客户机和服务器的范例。Web 客户机通过连接到一个支持 SSL 的服务器，启动一次 SSL 会话。支持 SSL 的典型 Web 服务器在一个与标准 HTTP 请求(默认为端口 80)不同的端口(默认为 443)上接受 SSL 连接请求。当客户机连接到这个端口上时，它将启动一次建立 SSL 会话的握手。当握手完成之后，通信内容被加密，并且执行消息完整性检查，直到 SSL 会话过期。

SSL 握手过程步骤。

步骤 1：SSL 客户机连接到 SSL 服务器，并要求服务器验证它自身的身份。

步骤 2：服务器通过发送它的数字证书证明其身份。这个交换还可以包括整个证书链，直到某个根证书权威企业(CA)，通过检查有效日期，确认证书可信任 CA 的数字签名，来验证证书。

步骤 3：服务器发出一个请求，对客户端的证书进行验证。但是因为缺乏公钥体系结构，当今的大多数服务器不进行客户端认证。

步骤 4：协商用于加密的消息加密算法和用于完整性检查的哈希函数。通常由客户机提供它支持的所有算法列表，然后由服务器选择最强健的加密算法。

步骤 5：客户机和服务器通过下列步骤生成会话密钥。

客户机生成一个随机数，并使用服务器的公钥(从服务器的证书中获得)对它加密，发送到服务器上。服务器用更加随机的数据(从客户机的密钥可用时则使用客户机密钥；否则以明文方式发送数据)响应。使用哈希函数，从随机数据生成密钥。

SSL 协议的优点是它提供了连接安全，具有 3 个基本属性：

① 连接是私有的。在初始握手定义了一个密钥之后，将使用加密算法。对于数据加密使用了对称加密(例如 DES 和 RC4)；

② 可以使用非对称加密或公钥加密(例如 RSA 和 DSS)来验证对等实体的身份;

③ 连接是可靠的。消息传输使用一个密钥的消息认证代码 MAC,包括了消息完整性检查。其中使用安全哈希函数(例如 SHA 和 MD5)来进行 MAC 计算。

HTTPS 协议基本知识

经常使用网上银行的朋友对“证书”这个词一定不会感到陌生,因为在登录网上银行的时候常常被要求验证数字证书。其实这是一个非常有效的安全措施,可以最大限度地保障用户的账户安全,而这种安全就是基于网络安全协议 HTTPS 协议(Secure Hypertext Transfer Protocol)来实现的。

HTTP 是超文本传输协议,信息在 Internet 上是明文传输,而 HTTPS 则是使用了具有安全性的 SSL 加密传输协议的 HTTPS 安全超文本传输协议,由网景公司开发并内置于其浏览器中,用于对数据进行压缩和解压操作,并返回网络上传送回反馈的结果。

WWW 服务是目前网络中最受欢迎的网络服务之一,它由 Web 服务器、Web 浏览器以及通信协议三部分组成。而 WWW 服务使用最多的就是超文本传输协议 HTTP(Hyper Text Transfer Protocol,HTTP),因此当用户浏览网页时可以在地址栏看到诸如 http://www. microsoft. com 形式的网址,其中最前面的 http 就表明该网站是基于 HTTP 通信。使用 HTTP 在 Web 服务器和 Web 浏览器之间传输数据时,HTTP 首先将 Web 浏览器的访问申请转换为 TCP/IP 支持的格式,并将该申请发送给 Web 服务器。Web 服务器通过 TCP/IP 接收到 Web 浏览器的申请后,将应答信息交给 HTTP,HTTP 经过处理返回给 Web 浏览器。在整个传输过程中数据都采用明文传输,因此很容易被黑客侦听和窃取。由此可见用 HTTP 在 Internet 上传输数据很不安全。

HTTPS 实际上应用了网景公司开发的安全套接字层 SSL 协议,作为 HTTP 应用层的子层,但 HTTPS 使用端口 443,而不是像 HTTP 那样使用端口 80 来和 TCP/IP 进行通信。SSL 使用 40 位关键字作为 RC4 流加密算法,适用于商业信息的加密。HTTPS 和 SSL 都支持使用 X. 509 数字认证,如果需要的话用户可以确认发送者身份。

使用 HTTPS 在 Internet 上传输数据时,发送方先把数据交给 SSL 协议进行加密,再把密文交由 TCP/IP 在网络上传输。接收方收到密文后,先提交给 SSL 协议解密成明文,然后再把明文进一步提交给 HTTP。在这个传输过程中,数据是使用密文的形式在网络中传输的,即使黑客窃取到传输的数据也不易破解,因此数据的安全性比较高。

HTTPS 是以安全为目标的 HTTP 通信,简单地讲是 HTTP 通信的安全版。即在 HTTP 通信中加入 SSL 安全协议,HTTPS 的安全基础是 SSL,用于安全的 HTTP 数据传输。https:URL 表明它使用了 HTTP,但 HTTPS 使用了不同于 HTTP 的默认端口及一个加密/身份验证层(在 HTTP 与 TCP 之间)。这个系统最初研发由网景公司进行,提供了身份验证与加密通信方法,现在它被广泛用于万维网上安全敏感通信,例如交易支付方面。

注意:SSL 是 HTTPS 的灵魂,HTTPS 的安全性来源于 SSL 加密算法。目前 SSL 使用一个由 Diffle 和 Hellman 提出的称为“公开密钥算法”的密码技术。此技术基于所谓

的密钥对,由两个不同的密钥构成一个密钥对。如果使用密钥对的一个密钥加密数据,它就只能用密钥对的另一个密钥解密。密钥对中的一个密钥是公开的,供用户用来加密数据,另一个则是私有的,用来对公开密钥加密的数据解密。

【实验原理】

锐捷 SSL VPN 采用 IP Tunnel 技术,除了能支持 B/S 应用,也能够支持各种 C/S 应用,对所有的基于 IP 层以上的静态或动态接口以及端口应用完全支持,包括网上邻居、文件共享、FTP,Outlook,SQL,Lotus NOTES,Sybase 和 Oracle 等各种应用。锐捷 SSL VPN 还支持终端用户对内网单台机器或保护子网的访问。这样公司员工无论在哪里,只要能够通过 Internet 登录网通总部 SSL VPN,即可访问内网服务器资源,从而达到正常处理公司业务的目的。

终端用户在使用 SSL VPN 的时候,不需要安装客户端,只需要通过标准浏览器打开 SSL VPN 的登录界面之后,安装一个 ActiveX 控件,在客户端的机器上会自动生成一块专门用于 SSL VPN 通信的虚拟网卡,从而保证 SSL VPN 的用户能够使用所有基于 IP 网络层的应用。

【实验步骤】

第一步：准备好 PC 和服务器

在服务器 PC 上安装 VPN 管理软件。

具体的安装过程不在这里进行详述。

第二步：搭建拓扑,配置 IP 地址

按照如图 4-88 所示拓扑图,搭建实验拓扑,并根据如表 4-3 所示编址方案,配置各设备的 IP 地址。

表 4-3 设备 IP 地址

设 备	接 口	地 址
VPN 网关	eth1 接口地址	192.168.1.1
	eth0 接口地址	10.1.1.1
PC	PC 的 IP 地址	192.168.2.1
	PC 网关地址	192.168.2.2
FTP 服务器	FTP 服务器 IP 地址	10.1.1.2
	FTP 服务器网关地址	10.1.1.1
Web 服务器	Web 服务器 IP 地址	10.1.1.3
	Web 服务器网关地址	10.1.1.1
远程桌面管理服务器	远程桌面管理服务器 IP 地址	10.1.1.4
	远程桌面管理服务器网关地址	10.1.1.1

续表

设　　备	接　　口	地　　址
Router	F0/0 地址	192.168.1.2
	F0/1 地址	192.168.2.2

说明：PC 及 Router 地址的配置方式不再详述。

通过服务器的超级终端，转入到命令行下配置 VPN 网关的接口地址，操作如图 4-89 所示。

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth0
Bring up onboot? (0: No, 1: Yes, Enter means Yes)

Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):

IP Address (xxx.xxx.xxx.xxx):
10.1.1.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.0.0.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)

Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):

IP Address (xxx.xxx.xxx.xxx):
192.168.1.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):

GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):
192.168.1.2
MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

Link-Guarantee Weight (1-255, Enter means 100):

[sadm@RG-WALL(Network)]#
```

图 4-89　配置 VPN 网关的接口地址

注意：VPN 网关出厂时 eth1 口默认地址为 192.168.1.1/24。并且在该实验中，需要在 VPN 网关的 eth1 接口配置默认网关，网关地址为 Router 的 F0/0 接口地址。

第三步：配置 SSL VPN 参数。

通过服务器上的 VPN 管理软件登录 VPN 网关。

(1) 资源的添加。

在 VPN 网关管理界面目录树中，单击“虚拟专用网”→“SSL VPN”选项，如图 4-90 所示。

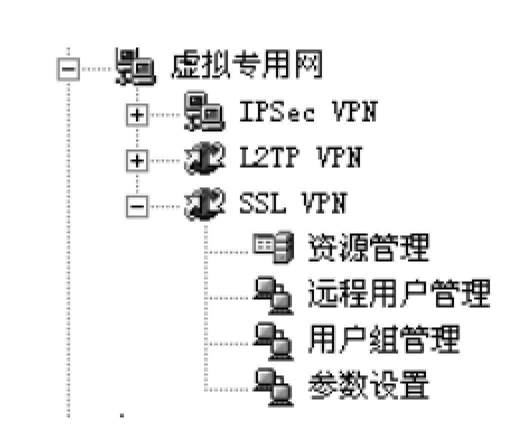


图 4-90　打开 SSL VPN 配置

选择“SSL VPN”菜单中“资源管理”项，进行 SSL VPN 资源添加，内网服务资源包括 FTP 服务资源、Web 服务资源、远程桌面管理资源。单击“资源管理”中的“添加资源”按钮，可以添加资源。如图 4-91 所示配置为添加内网 FTP 服务资源。

继续如图 4-92 所示配置，为添加内网 Web 服务资源。

继续如图 4-93 所示配置，为添加内网远程桌面管理服务资源。



图 4-91　添加内网 FTP 服务资源



图 4-92　添加内网 Web 服务资源



图 4-93　添加内网远程桌面管理服务资源

添加服务资源成功后，资源列表显示如图 4-94 所示。



序号	资源名	资源类型	资源地址	资源掩码	服务类型	资源端口	应用程序路径	程序参数
1	ftp服务	服务资源	10.1.1.2	255.255.255.255	FTP	TCP:20-21;1024-5000	NULL	NULL
2	web服务	服务资源	10.1.1.3	255.255.255.255	HTTP	TCP:80	NULL	NULL
3	远程桌面管理服务	服务资源	10.1.1.4	255.255.255.255	MSTSC	TCP:3389	NULL	NULL

图 4-94　成功添加服务资源

（2）远程用户管理。

在图 4-90 VPN 网关管理界面目录树中，选择“SSL VPN”，单击“远程用户管理”，弹出“远程用户管理”窗口，如图 4-95 所示。其中“本地认证数据库”中管理的用户就是网关本地用户，这些用户会自动出现在用户管理的本地认证数据库用户栏中。



图 4-95　配置远程用户管理

在“本地用户数据库”打开窗口中，添加本地用户 1a，该用户为 SSL VPN 登录用户，

添加 1a 用户，并设置相应的口令，其中口令自定义，如图 4-96 所示。

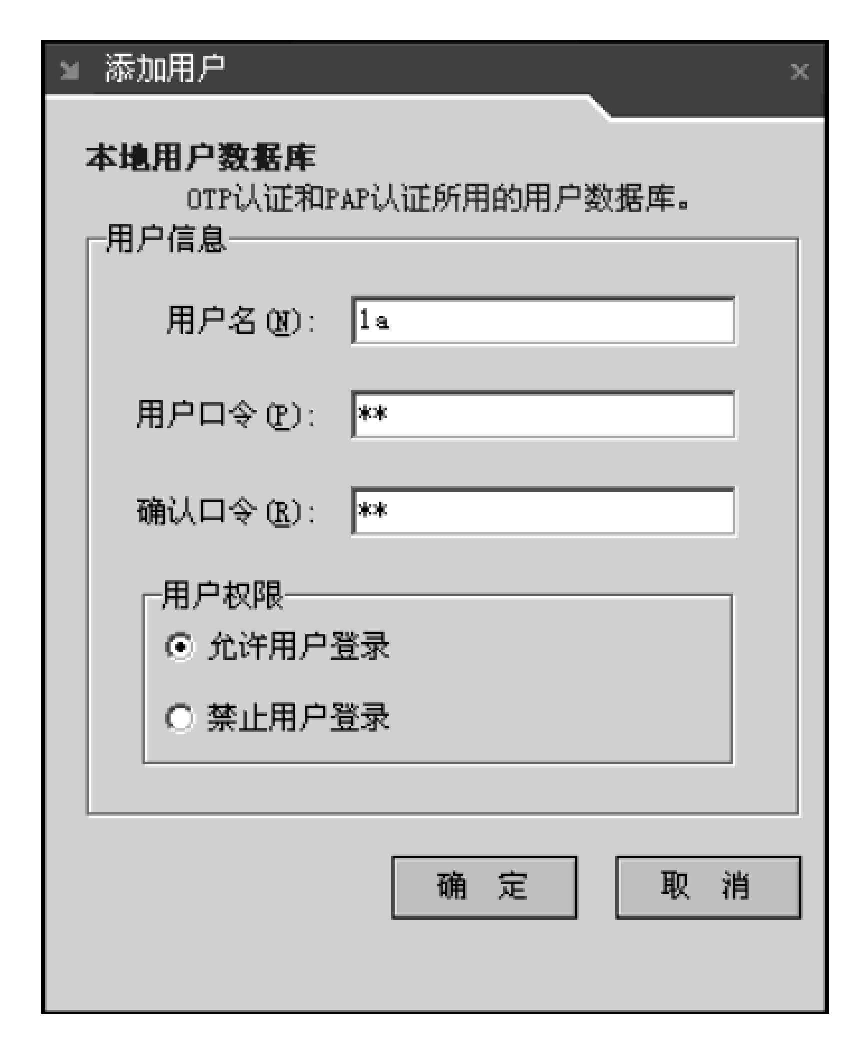


图 4-96 在本地用户数据库中添加本地用户

在本地用户数据库中添加本地用户添加成功后，如图 4-97 所示。

数据库生效 添加用户 删除用户 编辑用户 导入用户列表 导出用户列表

序号	用户权限	用户名	用户口令		权限	指定接口
1	普通用户	1a	******	✓	允许	ANY

图 4-97 成功在本地用户数据库中添加本地用户

在如图 4-95 所示的“远程用户管理”对话框中选择“用户管理”图标，把 1a 用户从本地数据库加入 SSL VPN 用户，如图 4-98 所示。



图 4-98 用户从本地数据库加入 SSL VPN

(3) 分配用户和资源。

在如图 4-90 所示 VPN 网关管理界面中，选择 SSL VPN→“用户组管理”项，打开“用户组管理”界面。用户组管理分为三大部分，添加用户组，为用户组分配用户和为用户组分配资源。添加一组名为 1 的用户组，如图 4-99 所示。

分配用户组用户资源成功后，如图 4-100 所示。

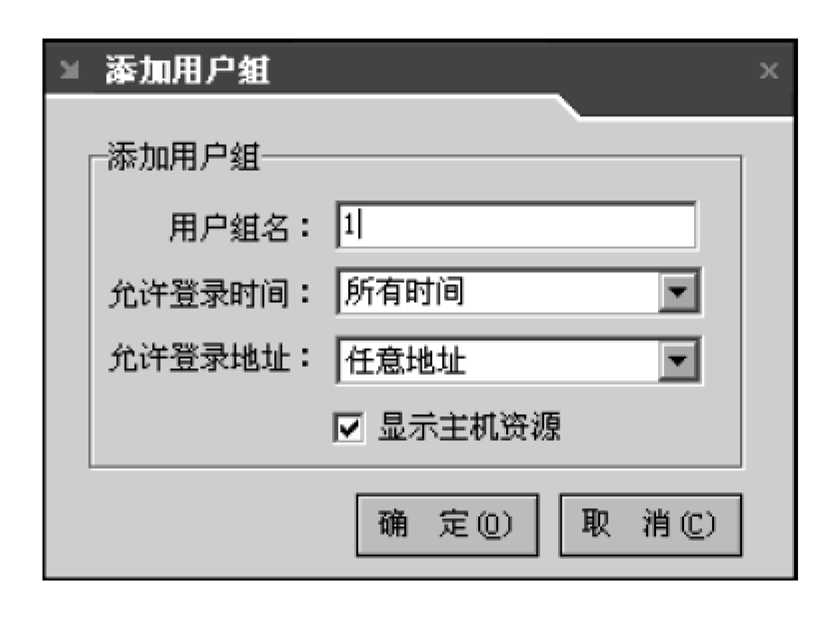


图 4-99 添加用户组资源

添加用户组 删除用户组 编辑用户组 时间对象 地址对象

序号	用户组名	时间对象名	地址对象名	显示主机资源
1	1	所有时间	任意地址	是

图 4-100 成功为用户组用户分配资源添加

选中如图 4-101 所示要进行分配用户的用户组，再单击工具栏中的“分配用户”按钮，就可以对选中的组进行用户分配，选中 1a 用户。

选中要进行分配用户的用户组，再单击工具栏中的“分配资源”按钮，可以为用户组分配已存在的资源，选中刚才添加的 3 个内网服务资源，如图 4-102 所示。



图 4-101 进行用户分配



图 4-102 添加内网服务资源

分配用户和添加内网服务资源成功后，如图 4-103 所示。

(4) SSL VPN 用户特征码设置。

在如图 4-90 所示 SSL VPN 管理菜单上选择“SSL VPN”项中“远程用户管理”项，在打开的“远程用户管理”对话框中选择“SSL 用户特征码表”，把用户接入策略由“禁止接入”改为“允许接入”，如图 4-104 所示。



图 4-103　成功分配用户和添加内网服务资源



图 4-104　修改用户接入策略

(5) 参数设置。

进入参数设置的工作界面中，如图 4-105 所示，可以进行如下操作。

① SSL 隧道设置：可设置 SSL 隧道通信协议的类型(目前主要支持协议为 UDP 和 TCP 方式)、SSL 隧道监听的端口、是否采用加密及验证算法；

② 虚 IP 地址池：这些地址将用于对登录 SSL VPN 的用户分配虚拟 IP 地址；

③ 连接超时：这个超时时间用于限制用户连续两次单击页面之间的间隔时间，如果用户在这个间隔时间内没有进行操作，网关会将其视为超时；

④ 定制界面：可以设置 Logo 图片及客户端浏览器的标题栏信息，如图 4-106 所示。

上述参数可以根据用户实际需求改变，一般情况下不需要更改，保持默认设置即可。

第四步：SSL VPN 用户登录。

(1) 插件与 SSL VPN 客户端程序的安装。

在验证 PC 的浏览器地址栏中输入 https://192.168.1.1，访问 SSL VPN 的登录页面。有三种登录方式，此实验只选择用户名口令方式登录。单击该方式，将出现如图 4-107 所示的登录提示框。



图 4-105 SSL 参数设置



图 4-106 设置 Logo 图片及客户端界面

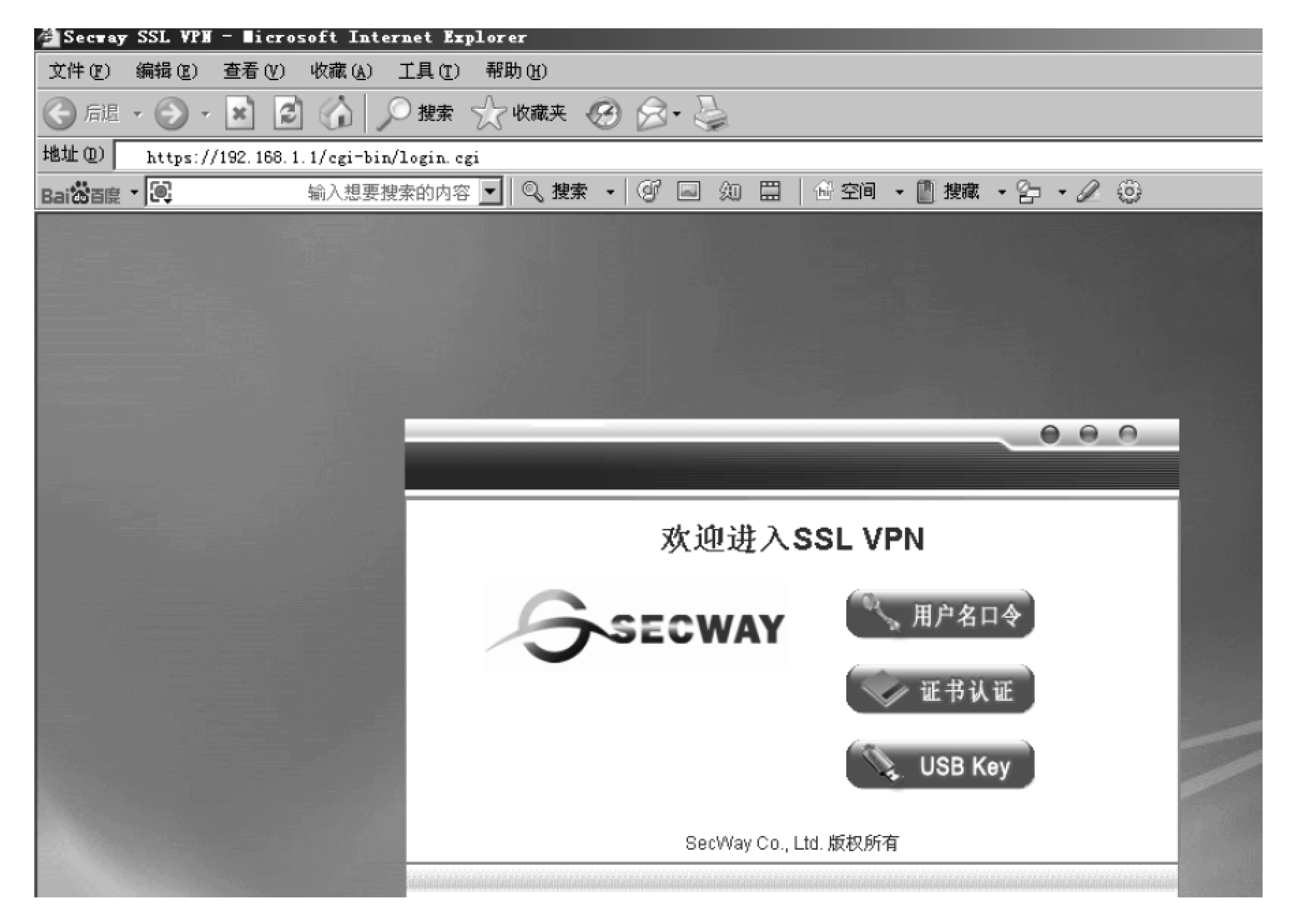


图 4-107 SSL VPN 的登录页面

如果首次使用 SSL VPN，输入用户 1a 正确的信息：用户名口令及验证码，单击登录，系统会自动安装插件和 SSL VPN 客户端，如图 4-108 所示。

正确登录后，系统提示安装插件和 SSL VPN 客户端，如图 4-109 所示。

弹出如下窗口时，单击“仍然继续”按钮，如图 4-110 所示。

完成 SSL VPN 客户端的安装。

(2) 内部资源的访问。

在安装完插件和 SSL VPN 客户端后，客户端登录成功，在浏览器的服务资源列表中



图 4-108　输入用户正确登录的信息

图 4-109　提示安装插件和客户端

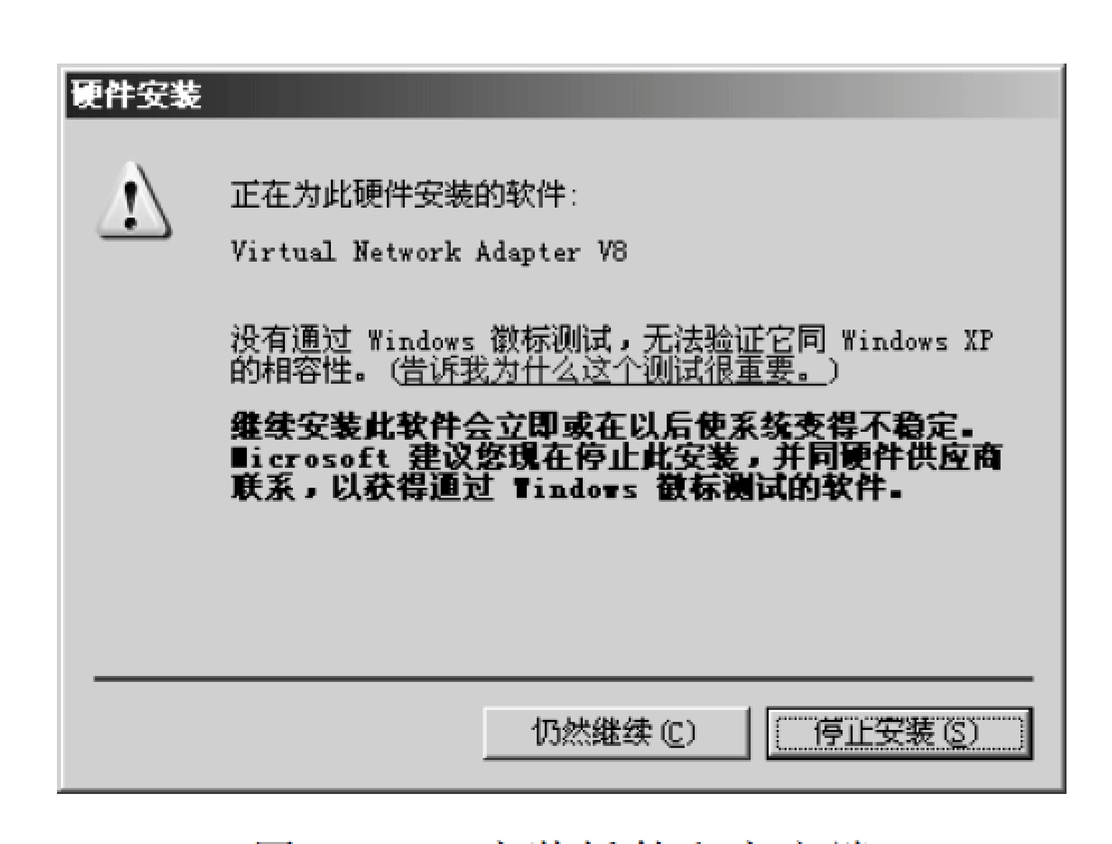


图 4-110　安装插件和客户端

可以看到能够访问的服务器资源，如图 4-111 所示。

内网 FTP 服务资源的访问：直接单击浏览器的服务资源列表中的“FTP 服务资源”，即可对内网 FTP 服务器进行下载、上传、删除等操作，如图 4-112 所示。

内网 Web 服务资源的访问：直接单击浏览器的服务资源列表中的“Web 服务资源”，

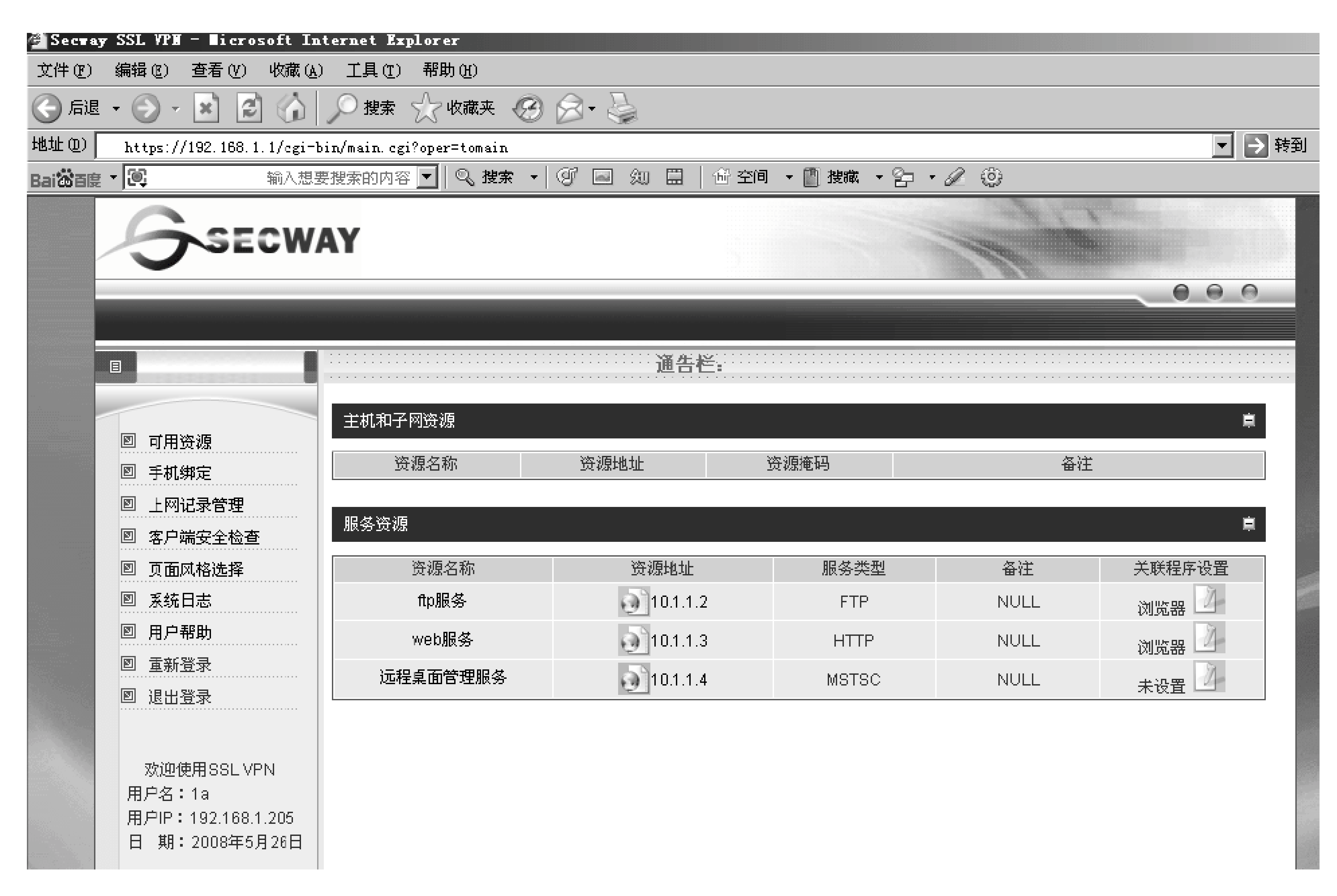


图 4-111 浏览器的服务资源列表中



图 4-112 内网 FTP 服务资源的访问

即可访问内网 Web 服务资源 10.1.1.3，如图 4-113 所示。

内网远程桌面管理服务资源的访问：在 Windows 系统 PC 上的远程桌面连接程序，在地址栏中输入 10.1.1.4，单击“连接”按钮，即可成功连接到需要访问和操作的内网服务器，如图 4-114 所示。

【注意事项】

- 在 IE 浏览器的 URL 地址栏中，必须输入 https://192.168.1.1，而非 http://192.168.1.1。
- 网关上“SSL VPN 用户特征码设置”选项默认配置为“禁止接入”，必须改为“允许接入”，否则客户端无法登录成功。

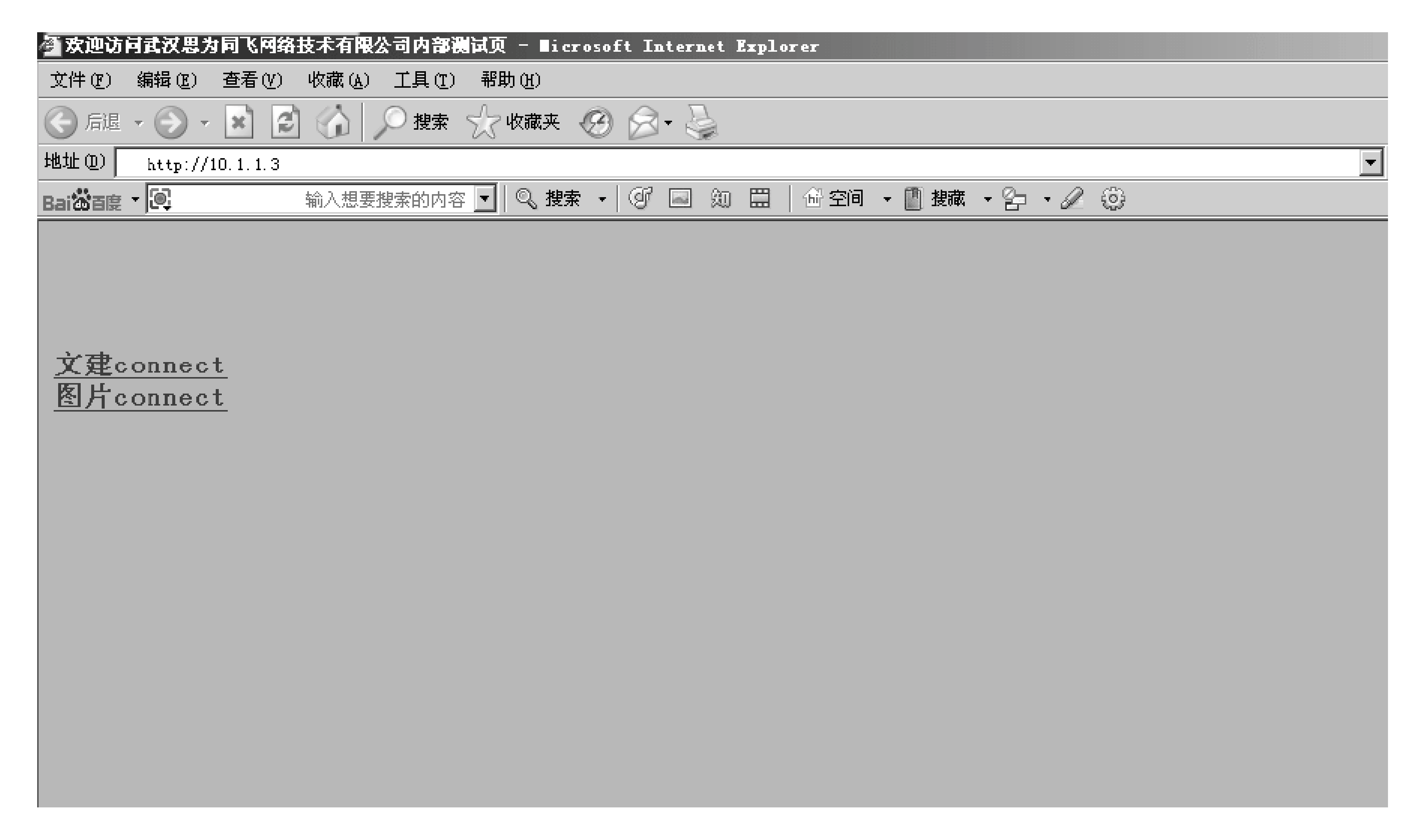


图 4-113　内网 Web 服务资源的访问

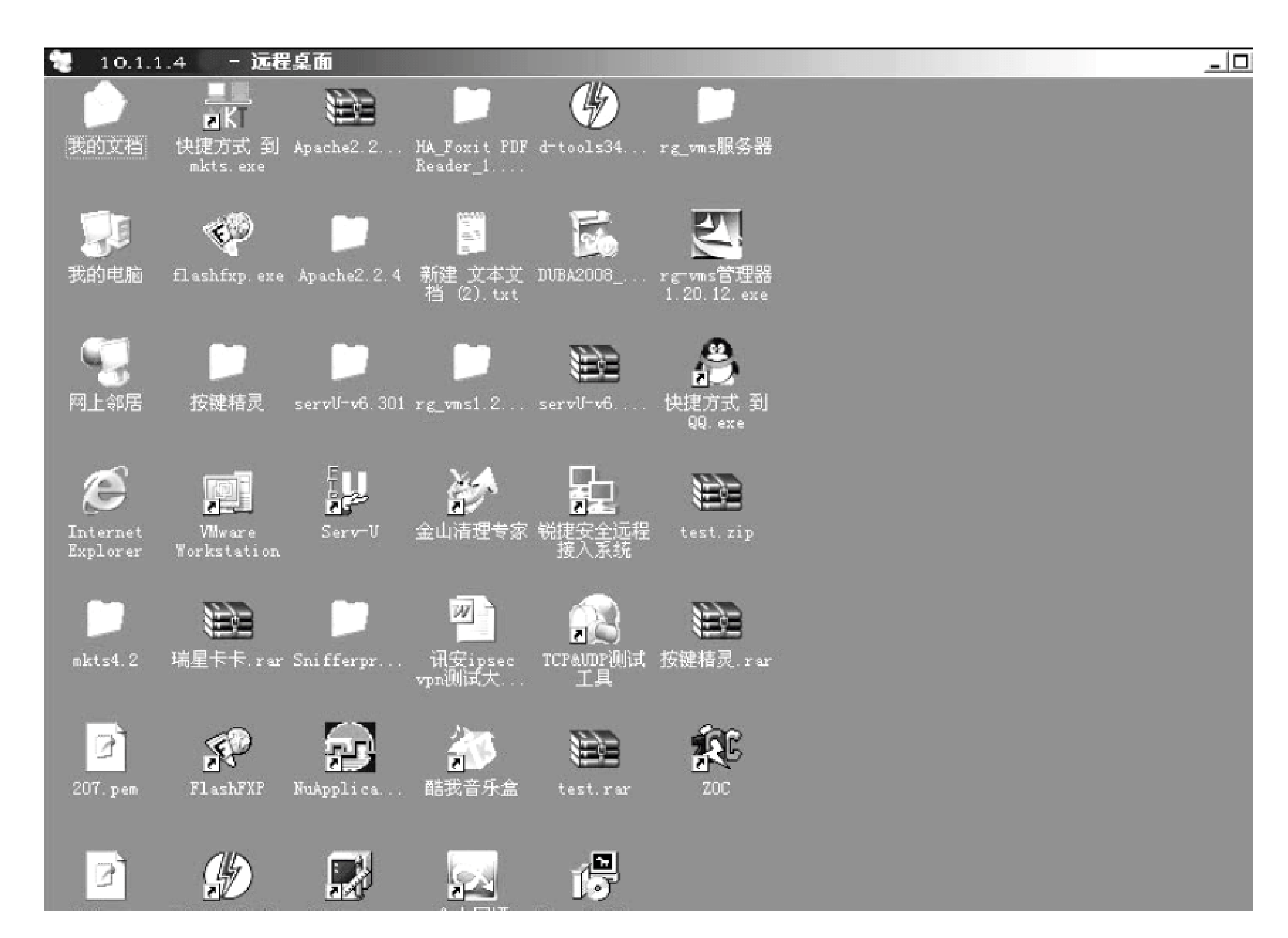


图 4-114　内网远程桌面管理服务资源的访问

- 客户端软件安装过程中，弹出如图 4-115 所示“硬件安装”提示窗口，必须单击“仍然继续”按钮，否则客户端登录不成功。
- 如出现客户端或插件无法自动安装，请检查客户端 PC 是否因为防火墙阻止了其安装。
- 如发现客户端登录后访问资源不成功，且客户机任务管理器中无 sslvpn.exe 进程，请卸载 SSL VPN 客户端后重新安装。
- 在网关本地数据库中添加用户后，必须单击“用户生效”按钮，否则用户无法登录 SSL VPN。

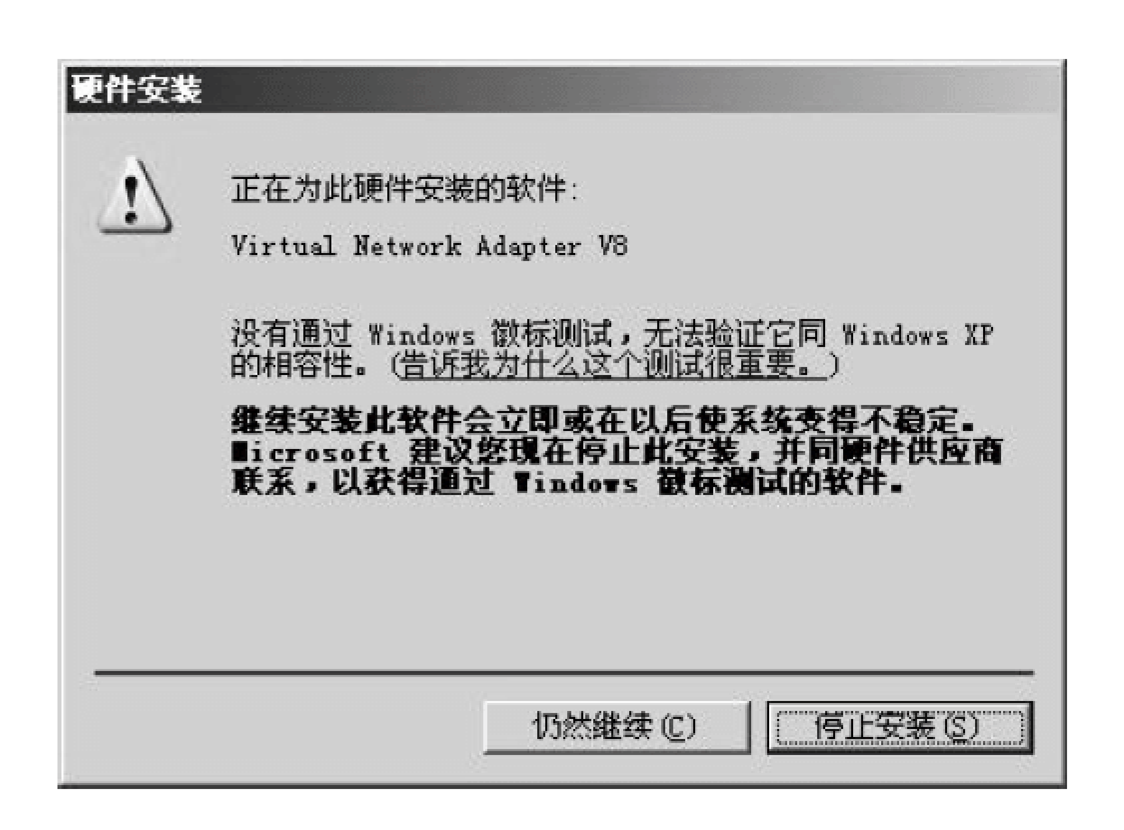


图 4-115 “硬件安装”提示窗口

4.4 构建 SSL VPN 单臂通信实验

【实验名称】

构建 SSL VPN 单臂通信。

【实验目的】

学习配置 SSL VPN 隧道、掌握 SSL VPN 单臂方式接入拓扑，加深对 SSL VPN 的理解。

【背景描述】

某公司内部网络结构以及 IP 划分极为复杂，该公司希望在不改变现在网络拓扑的情况下，在局域网内部以单臂路由方式接入一台 SSL VPN 设备，使得外网用户通过登录该设备来访问公司内部资源。

【需求分析】

需求：在不改变现有网络拓扑情况下，单臂方式接入 SSL VPN，使得外网用户登录并且通过该设备访问内部资源。

分析：SSL VPN 采用 IP Tunnel 技术，支持 B/S 应用，也支持各种 C/S 应用，对所有基于 IP 层以上静态或动态接口以及端口应用完全支持，包括网上邻居、文件共享、FTP、Outlook、SQL、Lotus Notes、Sybase、Oracle 等各种应用。锐捷 SSL VPN 还支持终端用户对内网单台机器或受保护子网的访问。

终端用户在使用锐捷 SSL VPN 的时候，不需要安装客户端程序，只需要通过标准浏览器打开 SSL VPN 的登录界面之后，从而保证锐捷 SSL VPN 的用户能够使用所有基于 IP 网络层的应用。使用 SSL VPN 网关与自身防火墙功能结合，实现单臂路由方式。

【实验拓扑】

如图 4-116 所示网络拓扑，是某公司上海分公司内部网络。公司内部网络结构以及

IP 规划极为复杂，公司希望在不改变现在网络拓扑的情况下，在局域网内部以单臂路由方式接入一台 SSL VPN 设备，使得外网用户通过登录该设备来访问公司内部资源，实现分公司和总公司之间信息共享。

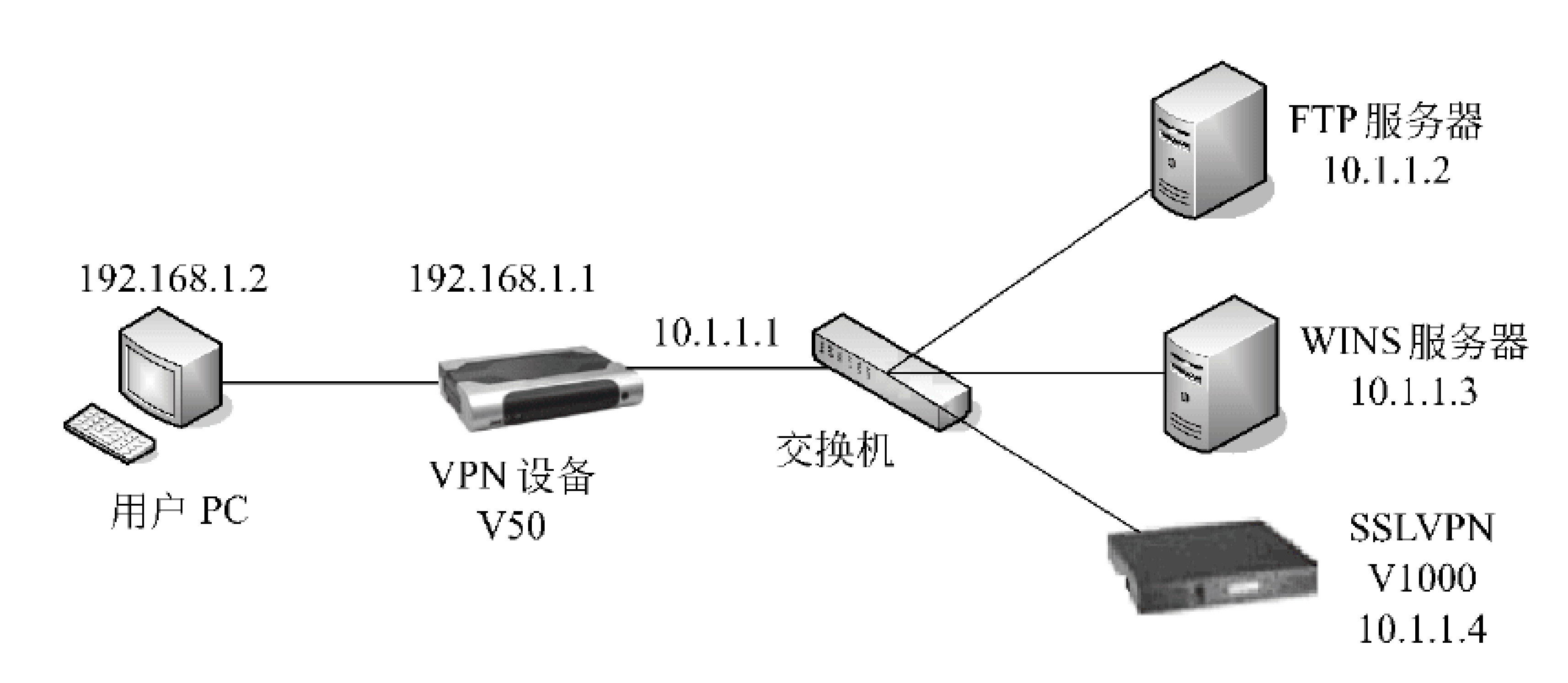


图 4-116 构建 SSL VPN 单臂通信网络拓扑

为解决上海分公司和北京总公司之间，通过 Internet 进行数据传输的安全问题。公司希望通过 VPN 技术，不改变现有网络拓扑，单臂方式接入 SSL VPN，使得外网用户登录并且通过该设备访问内部资源，有效保证数据在 Internet 网络传输的安全问题。

【实验设备】

RG-WALL V1000 VPN 网关：1 台；RG-WALL V50 VPN 网关：1 台；交换机：1 台；PC：3 台；直连线：2 根；交叉线：2 根。

【实验原理】

用户在 Windows 系统 PC 上访问 SSL VPN 指定站点，通过特定的登录方式登录 SSL VPN，安装相关的系统插件和 SSV LPN 客户端，登录成功后用户和 VPN 设备之间会建立 SSL VPN 加密隧道，从而实现访问 VPN 内网资源的目的。

【实验步骤】

第一步：准备好 PC 和服务器。

在服务器 PC 上安装 VPN 管理软件(见随机附带的光盘，此处不再详述)。

第二步：搭建拓扑，配置 IP 地址。

按照如图 4-116 所示拓扑图，搭建实验拓扑，并根据如表 4-4 所示编址方案，配置各设备的 IP 地址。

表 4-4 设备 IP 地址

设 备	接 口	地 址
V50 VPN 网关	eth1 接口地址	192.168.1.1
	eth0 接口地址	10.1.1.1
V1000 VPN 网关	eth1 接口地址	10.1.1.4
	eth0 接口地址	10.1.1.1

续表

设　　备	接　　口	地　　址
PC	PC 的 IP 地址	192.168.1.2
	PC 网关地址	192.168.1.1
FTP 服务器	服务器的 IP 地址	10.1.1.2
	服务器网关地址	10.1.1.1
Web 服务器	服务器的 IP 地址	10.1.1.3
	服务器网关地址	10.1.1.1

说明：PC 及 Router 地址的配置方式不再详述。

(1) 通过 PC 的超级终端，在命令行下配置 VPN 设备 V50 VPN 的 eth1 口地址，操作如图 4-117 所示。

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manu
al):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.1.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]# _
```

图 4-117　配置 V50 VPN 网关的接口地址

注意：VPN 出厂时 eth1 口默认地址即为 192.168.1.1，因此可以先查看接口配置，如果的确如此，则可以免去该配置步骤。

(2) 通过 PC 上的 VPN 管理软件登录 VPN 设备 V50 VPN，选择管理界面上“网络接口”项，然后选择“eth0 口”图标，双击打开配置 eth0 口地址，如图 4-118 所示。

在打开的“eth0 口”对话框中，设置 eth0 口地址，如图 4-119 所示。

(3) 验证测试。

通过 PC 可以 ping 通 VPN 设备 V50 VPN 的 eth1 口；

通过 VPN 设备 V50 VPN 可以 ping 通 FTP 和 Web 服务器。

第三步：按照搭建拓扑，配置 V1000 VPN 网关 IP 地址。

通过 PC 的超级终端，在命令行下配置 VPN 设备 V1000 VPN 的 eth1 口地址，操作如图 4-120 所示。

第四步：SSL VPN 参数配置。

登录网关 10.1.1.4 地址的 V1000 VPN，配置其 SSL VPN 各项参数信息。

(1) 资源的添加。

在登录网关 10.1.1.4 地址的 V1000 VPN 网关管理界面目录树中，单击“虚拟专用

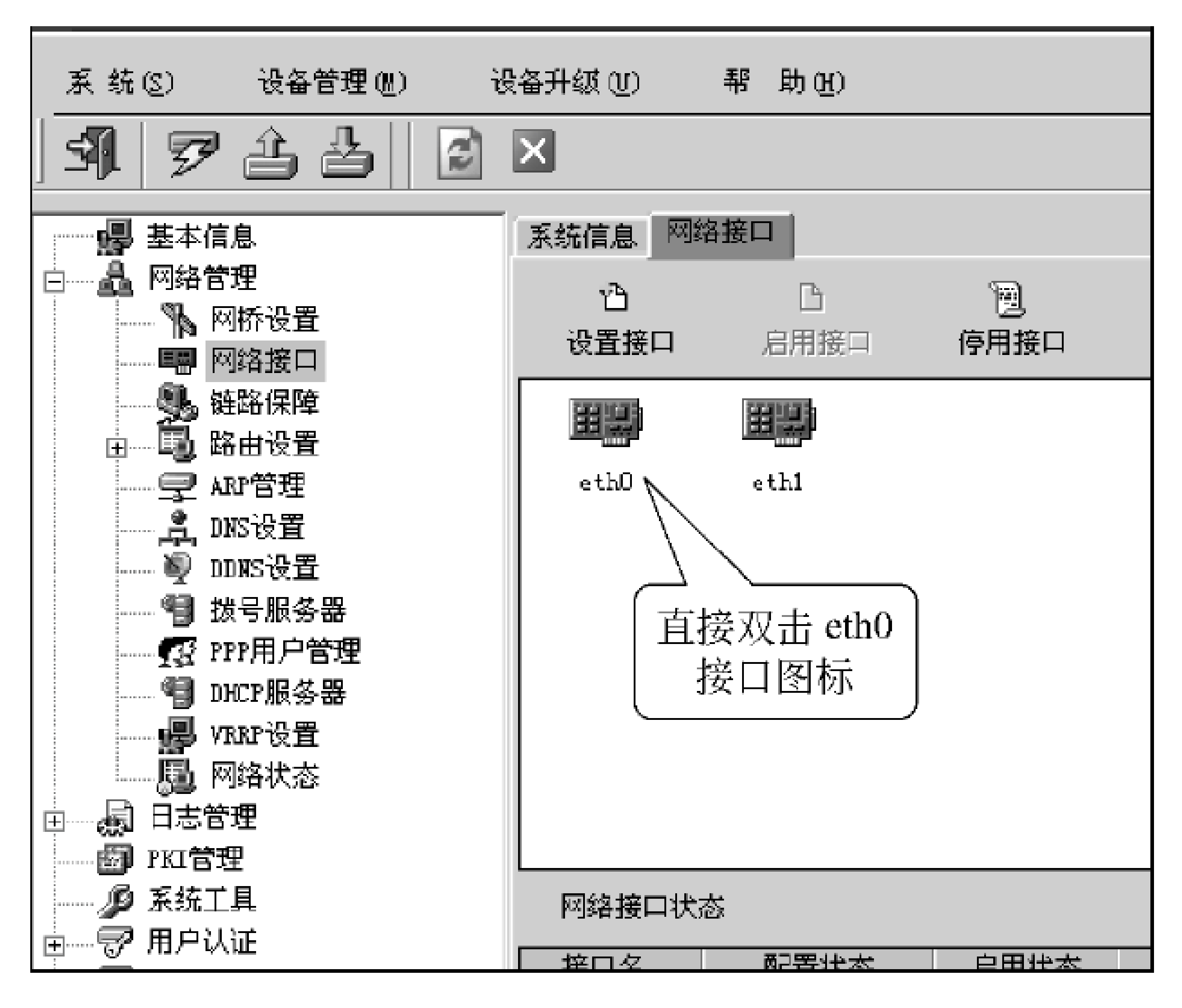


图 4-118　配置 VPN 网关 V50 VPN 的接口地址



图 4-119　配置 VPN 网关 V50 VPN 的接口地址

```
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth0
Bring up onboot? (0: No, 1: Yes, Enter means Yes)

Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):

IP Address (xxx.xxx.xxx.xxx):
10.1.1.4
Netmask (xxx.xxx.xxx.xxx, Enter means 255.0.0.0):

GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):
10.1.1.1
MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

Link-Guarantee Weight (1-255, Enter means 100):
```

图 4-120　配置 V1000 VPN 的 eth1 口地址

网”→SSL VPN，如图 4-121 所示。

在如图 4-121 所示的界面上，选择 SSL VPN 下拉栏“资源管理”项中进行 SSL VPN 资源添加，内网服务资源包括 FTP 服务资源、Web 服务资源、远程桌面管理资源。

单击“资源管理”工具栏中“添加资源”按钮，可以添加资源。如图 4-122 所示，配置添加内网 FTP 服务资源。

如图 4-123 所示，配置添加内网 Web 服务资源。



图 4-121　SSL VPN 参数配置



图 4-122　添加资源



图 4-123　配置内网 Web 服务资源

图 4-124 所示为添加成功后资源列表。

添加资源　删除资源　编辑资源　资源上移　资源下移

序号	资源名	资源类型	资源地址	资源掩码	服务类型	资源端口	应用程序路径	程序参数
1	ftp服务	服务资源	10.1.1.2	255.255.255.255	FTP	TCP:20-21;1024-5000	NULL	NULL
2	web服务	服务资源	10.1.1.3	255.255.255.255	HTTP	TCP:80	NULL	NULL
3	远程桌面管理服务	服务资源	10.1.1.4	255.255.255.255	MSTSC	TCP:3389	NULL	NULL

图 4-124　添加成功后资源列表

(2) 远程用户管理。

在如图 4-121 所示界面上，选择“SSL VPN”下拉栏中“远程用户管理”项，打开“远程用户管理”窗口，如图 4-125 所示。



图 4-125　远程用户管理

“本地认证数据库”中用户就是网关本地用户，打开“远程用户管理”中“本地用户数据库”，这些用户会自动出现在用户管理的本地认证数据库用户栏中。

在打开的“本地用户数据库”中，添加本地用户 1a，该用户为 SSL VPN 登录用户，添加用户名为 1a 用户，并设置相应的口令，口令自定义，如图 4-126 所示。

添加本地用户 1a 成功后，如图 4-127 所示。

在如图 4-125 所示“远程用户管理”界面上，在“远程用户管理”对话框中，打开“用户管理”项，把 1a 用户从本地数据库添加到 SSL VPN 用户中，如图 4-128 所示。

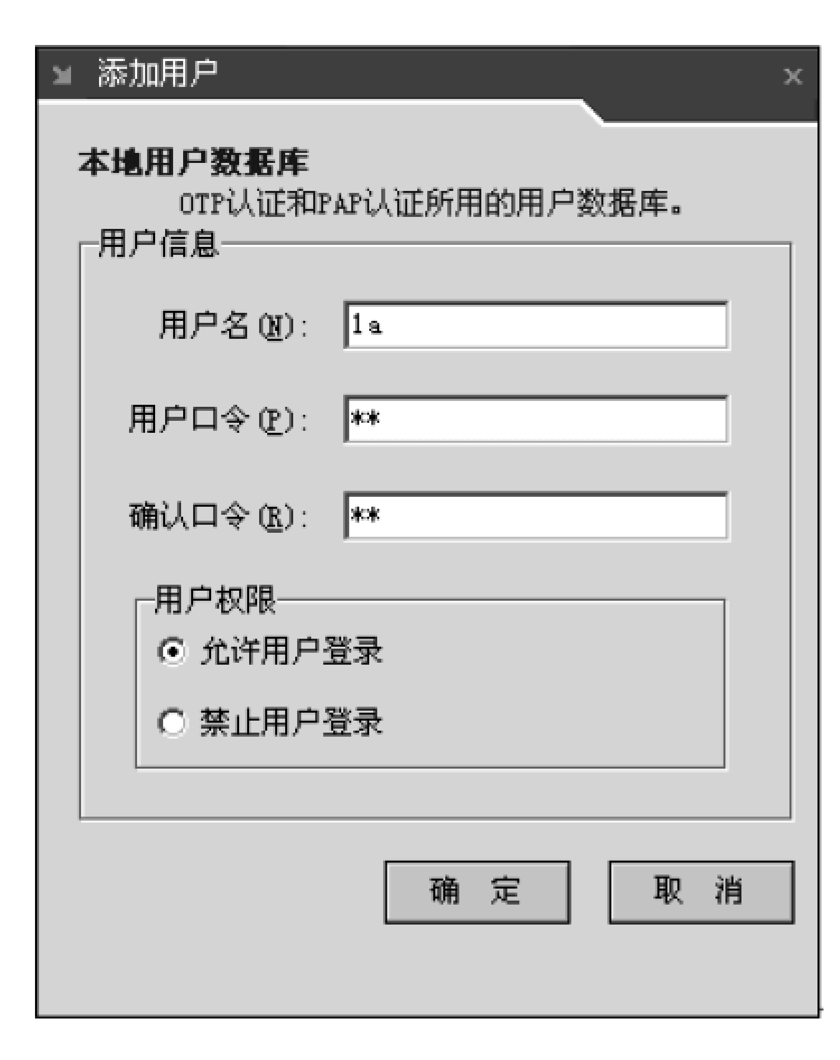


图 4-126　添加本地用户

(3) 分配用户和资源。

在如图 4-121 所示登录网关 10.1.1.4 地址 V1000 VPN 网关管理界面中，选择“虚拟专用网”→SSL VPN。

数据库生效　添加用户　删除用户　编辑用户　导入用户列表　导出用户列表

序号	用户权限	用户名	用户口令	权限	指定接口
1	普通用户	1a	******	✔ 允许	ANY

图 4-127　添加本地用户成功

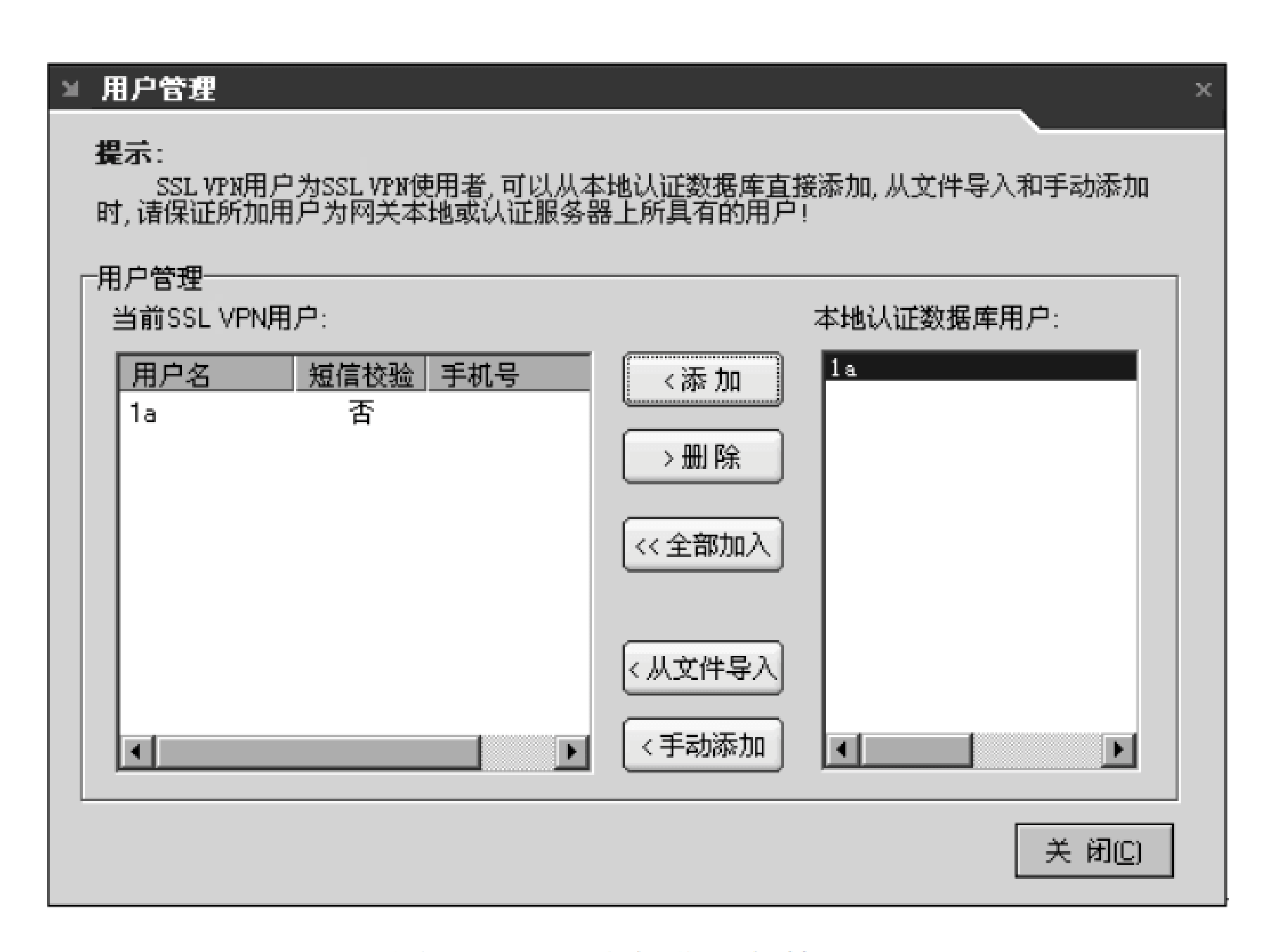


图 4-128　选择“用户管理”

在目录树上选中“用户组管理”项，打开“添加用户组”管理界面，如图 4-129 所示，用户组管理分为三大部分：添加用户组，为用户组分配用户和为用户组分配资源。如

图 4-129 所示，为“用户组管理”添加一名字为 1 的用户组。

添加成功后，如图 4-130 所示。

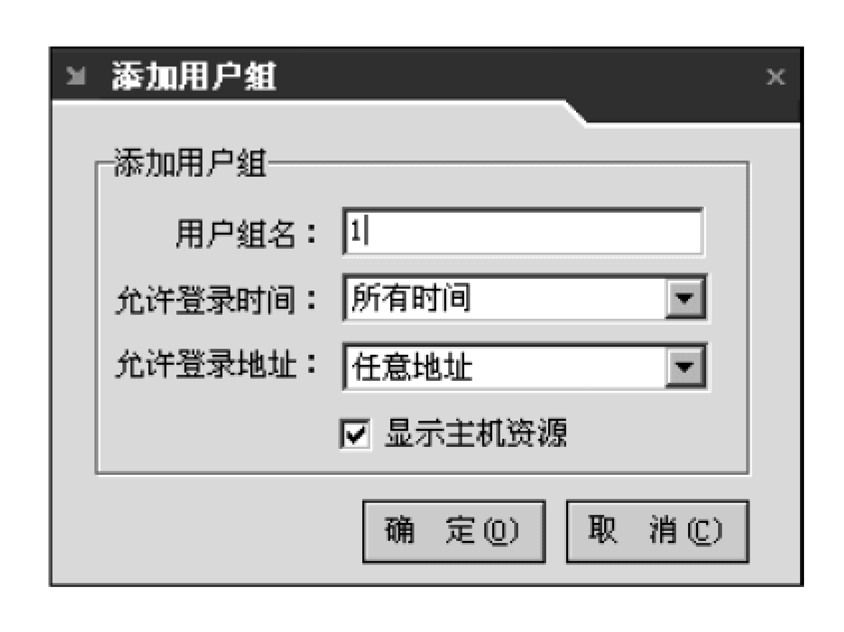


图 4-129 添加用户组

添加用户组 删除用户组 编辑用户组 时间对象 地址对象

序号	用户组名	时间对象名	地址对象名	显示主机资源
1	1	所有时间	任意地址	是

图 4-130 用户组添加成功

在如图 4-130 所示界面上，选中要进行分配用户的用户组，再单击工具栏中的“分配用户”按钮，就可以对选中的组进行用户分配，选中 1a 用户，如图 4-131 所示。

在如图 4-131 所示界面上，选中要进行分配用户的用户组，再单击工具栏中的“分配资源”按钮，可以为用户组分配已存在的资源，选中刚才添加的 3 个内网服务资源，如图 4-132 所示。



图 4-131 选择用户组分配资源



图 4-132 用户组分配资源成功

如图 4-133 所示界面为分配用户和资源成功后。

(4) SSL VPN 用户特征码设置。

在图 4-125 所示“远程用户管理”对话框中，选择“SSL 用户特征码表”项，把用户接入策略由“禁止接入”改为“允许接入”，如图 4-134 所示。

(5) 参数设置。

在如图 4-125 所示“远程用户管理”界面上，选择“认证参数”项，在打开参数设置的工作界面中，如图 4-135 所示，可以进行如下操作。

① SSL 隧道设置：可设置 SSL 隧道通信协议的类型，目前主要支持协议为 UDP 和 TCP 方式，SSL 隧道监听的端口，是否采用加密及验证算法；

② 虚 IP 地址池：将用于对登录 SSL VPN 的用户分配虚拟 IP 地址；

③ 连接超时：用于限制用户连续两次单击页面之间的间隔时间，如果用户在这个间



图 4-133　分配用户和资源成功分配



图 4-134　选择“SSL 用户特征码表”

隔时间内没有进行操作，网关会将其视为超时。

在如图 4-135 所示界面上，选择“定制界面”项，可以设置 Logo 图片及客户端浏览器的标题栏信息，如图 4-136 所示。

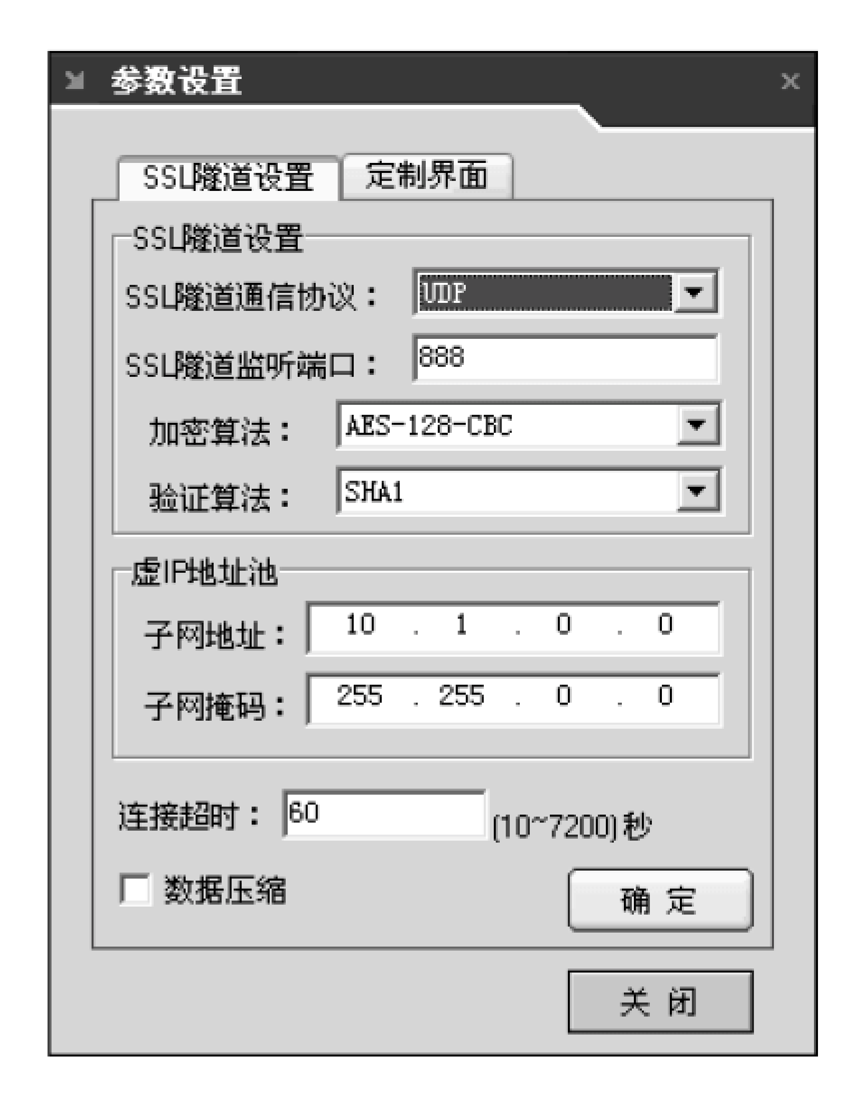


图 4-135　选择“认证参数”



图 4-136　选择“定制界面”

上述参数根据用户实际需求改变，一般情况不需要更改，保持默认设置即可。

(6) 配置 VPN 设备 V1000 VPN 地址转换 NAT 参数。

登录网关 10.1.1.4 地址的 V1000 VPN 网关，在打开的目录树管理界面中，单击“防火墙”→“新建防火墙规则”，配置如图 4-137 所示的信息。

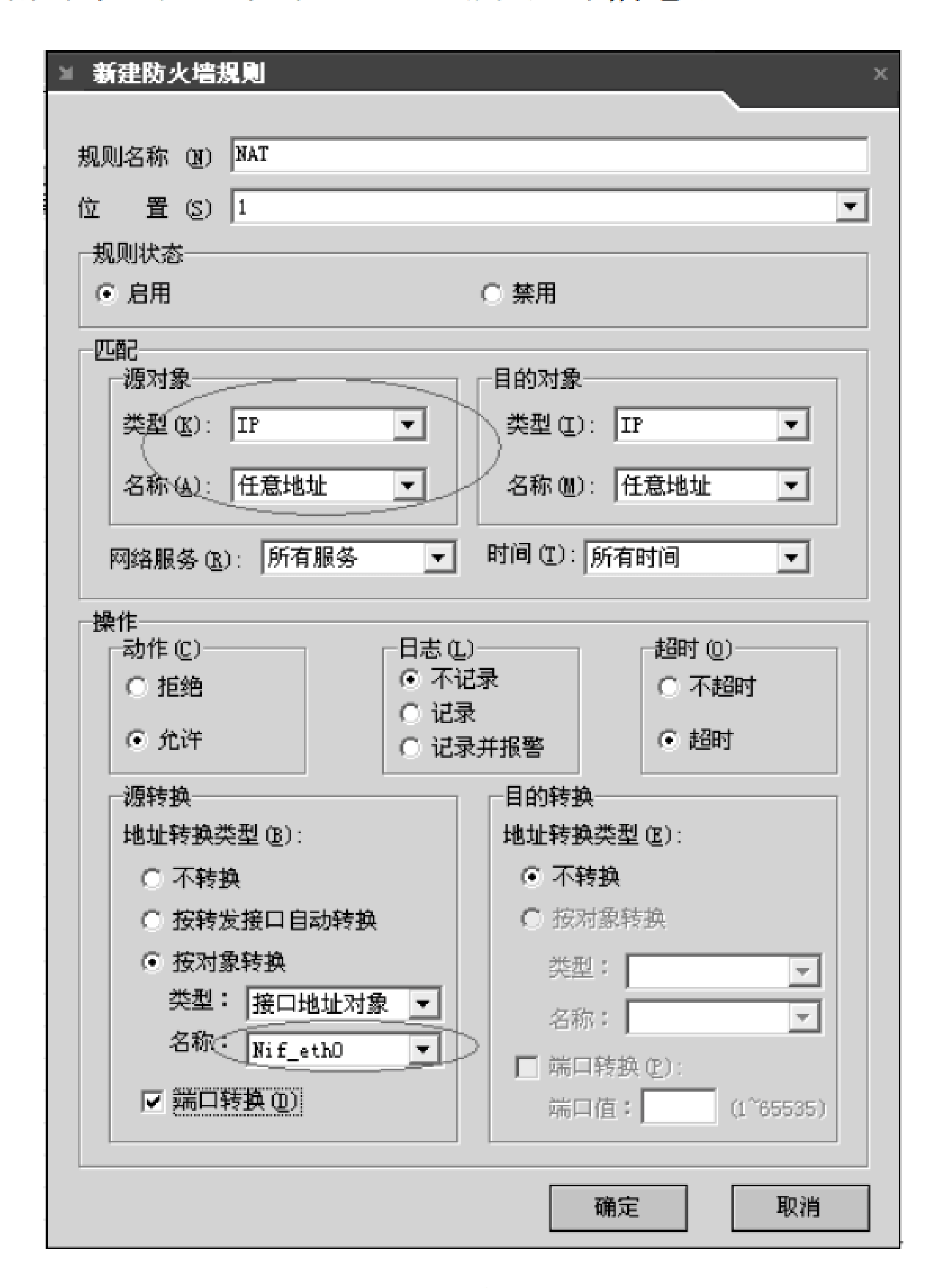


图 4-137　新建防火墙规则

登录网关 10.1.1.4 地址的 V1000 VPN 网关，在打开的目录树管理界面中，单击“防火墙”→“安全参数”，如图 4-138 所示配置。



图 4-138　配置防火墙规则参数

(7) 配置 VPN 设备 V50 VPN 地址转换 MAP 映射。

打开 V50 VPN 设备,登录管理界面,在 VPN 设备 V50 上配置 MAP 映射,使得外网用户能通过映射登录 VPN 设备 V1000。

登录 V50 VPN 网关,在打开的目录树管理界面中,单击"防火墙"→"安全参数",首先选择"IP 地址对象",打开"添加 IP 地址对象成员"对话框,在打开的防火墙 IP 地址对象中,添加 VPN 设备 V1000 的 IP 地址,如图 4-139 所示。然后在"转换地址对象"中,双击打开"添加转换地址对象成员"对话框,添加 192.168.1.0 网段内一任意空闲 IP 地址,作为 10.1.1.4 的映射地址,如 192.168.1.4,如图 4-140 所示。

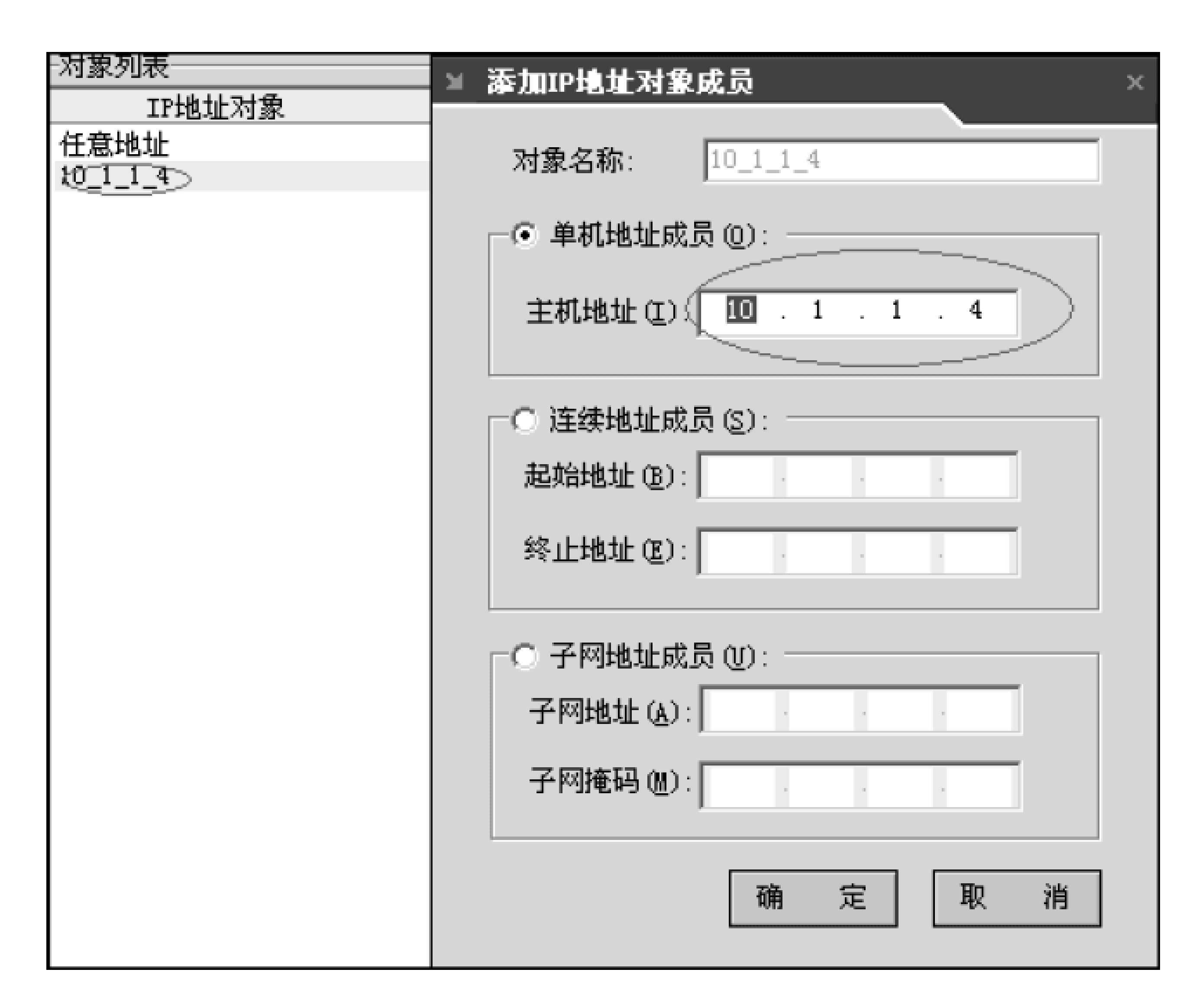


图 4-139 添加 VPN 设备 V1000 的 IP 地址

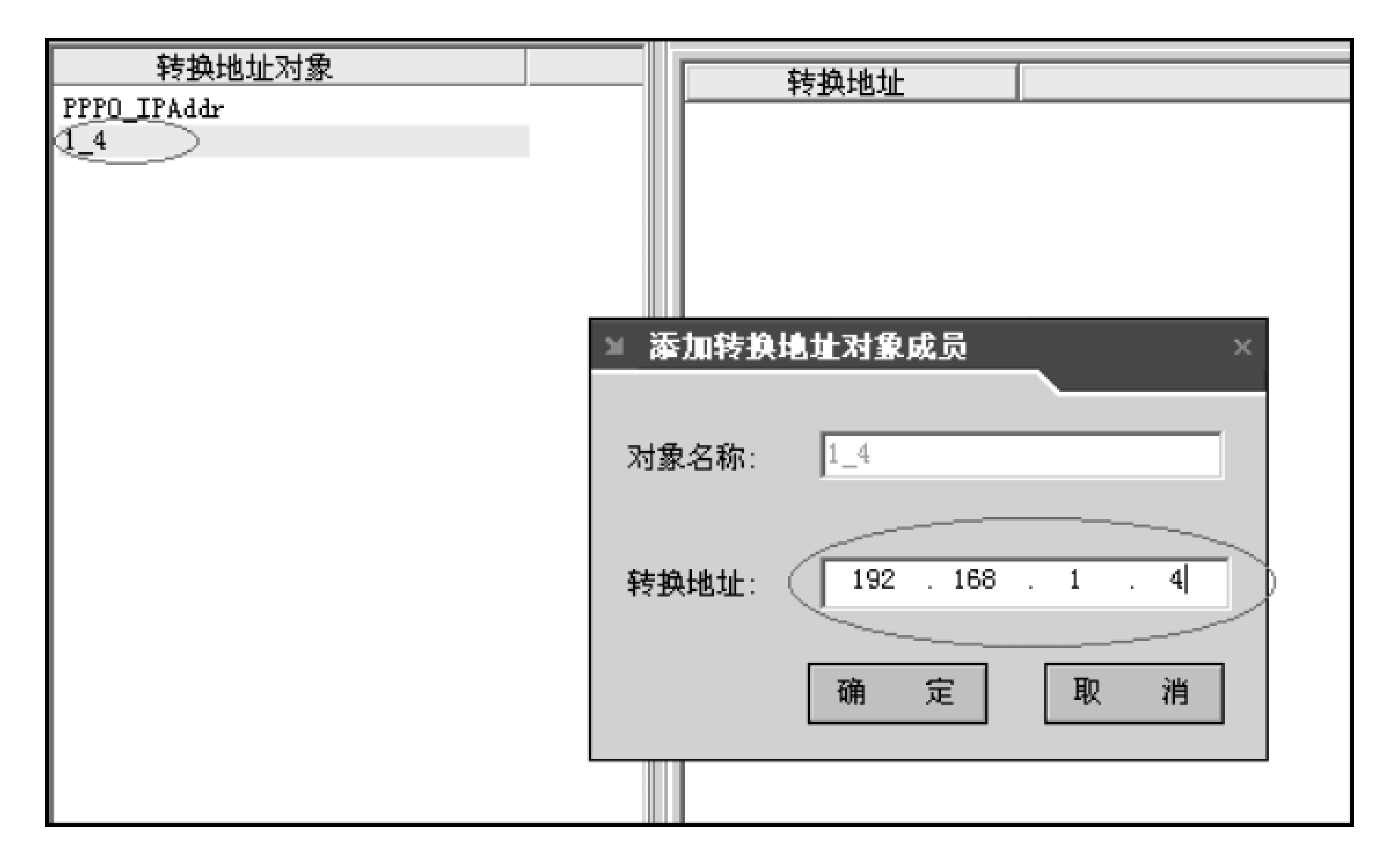


图 4-140 添加转换地址对象成员

登录 V50 VPN 网关,在打开的目录树管理界面中,单击"防火墙"→"新建防火墙规则",最后配置防火墙 MAP 映射规则,如图 4-141 所示。

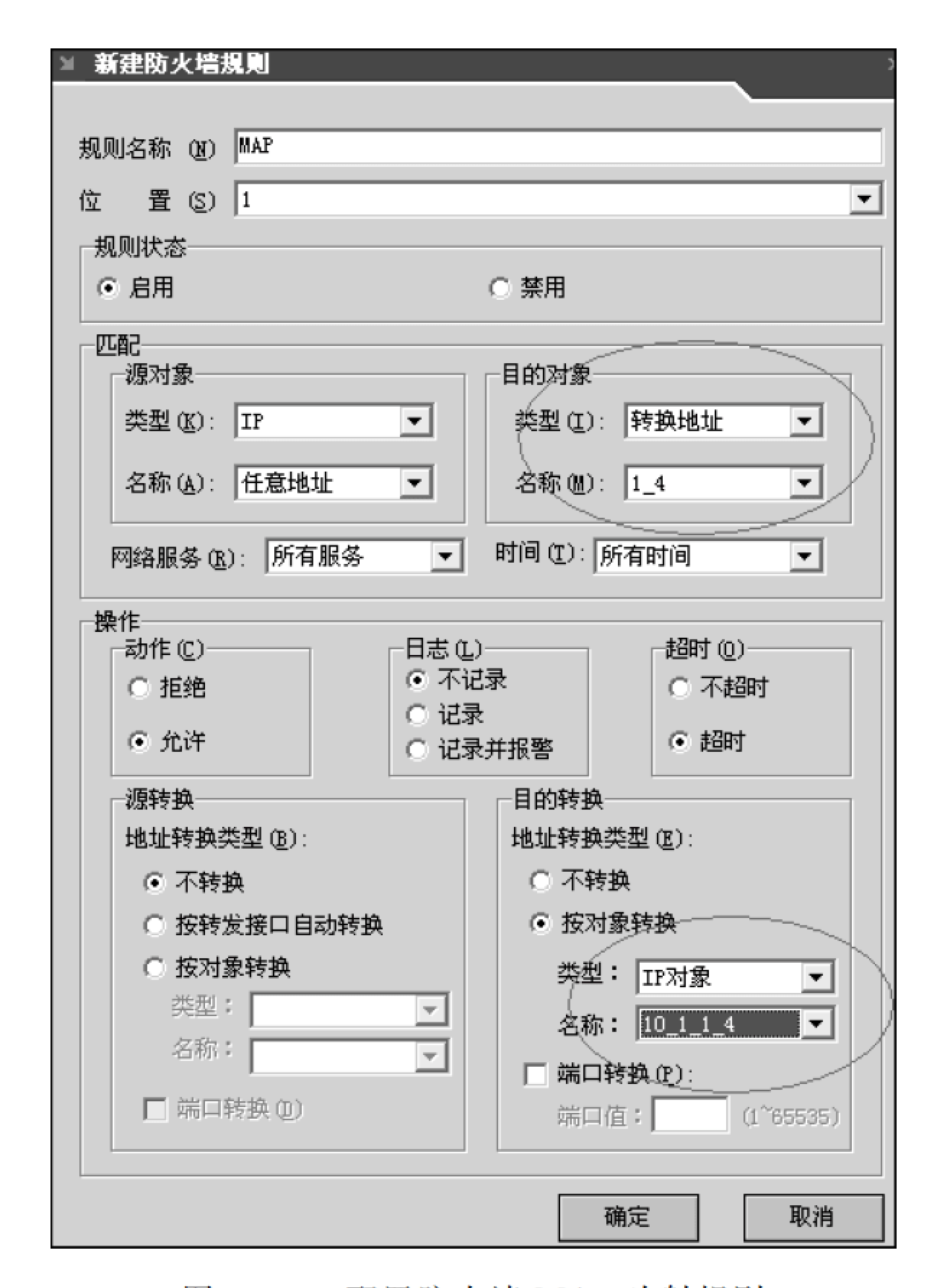


图 4-141　配置防火墙 MAP 映射规则

第五步：SSL VPN 用户登录。

(1) 为客户端设备安装插件与 SSL VPN 客户端程序的安装。

在接入 PC 的浏览器地址栏中，输入登录 https://192.168.1.4，访问 SSL VPN 的登录页面。提供有三种登录方式，此实验只选择“用户名口令”方式登录。单击该方式，将出现如图 4-142 所示的登录提示框。

如果首次使用 SSL VPN，输入用户 1a 正确的用户名口令及验证码，单击“登录”，系统会自动安装插件和 SSL VPN 客户端，如图 4-143 所示。

安装插件和 SSL VPN 客户端，如图 4-144 所示。

弹出如下窗口时，单击“仍然继续”按钮，如图 4-145 所示，即可完成 SSL VPN 客户端的安装。

(2) 内部资源的访问。

安装完插件和 SSL VPN 客户端后，客户端登录成功，在浏览器的服务资源列表中可以看到能够访问的服务器资源，如图 4-146 所示。

(3) 内网 FTP 服务资源的访问。

直接单击浏览器的服务资源列表中的“ftp 服务资源”，即可对内网 FTP 服务器进行下载、上传、删除等操作，如图 4-147 所示。

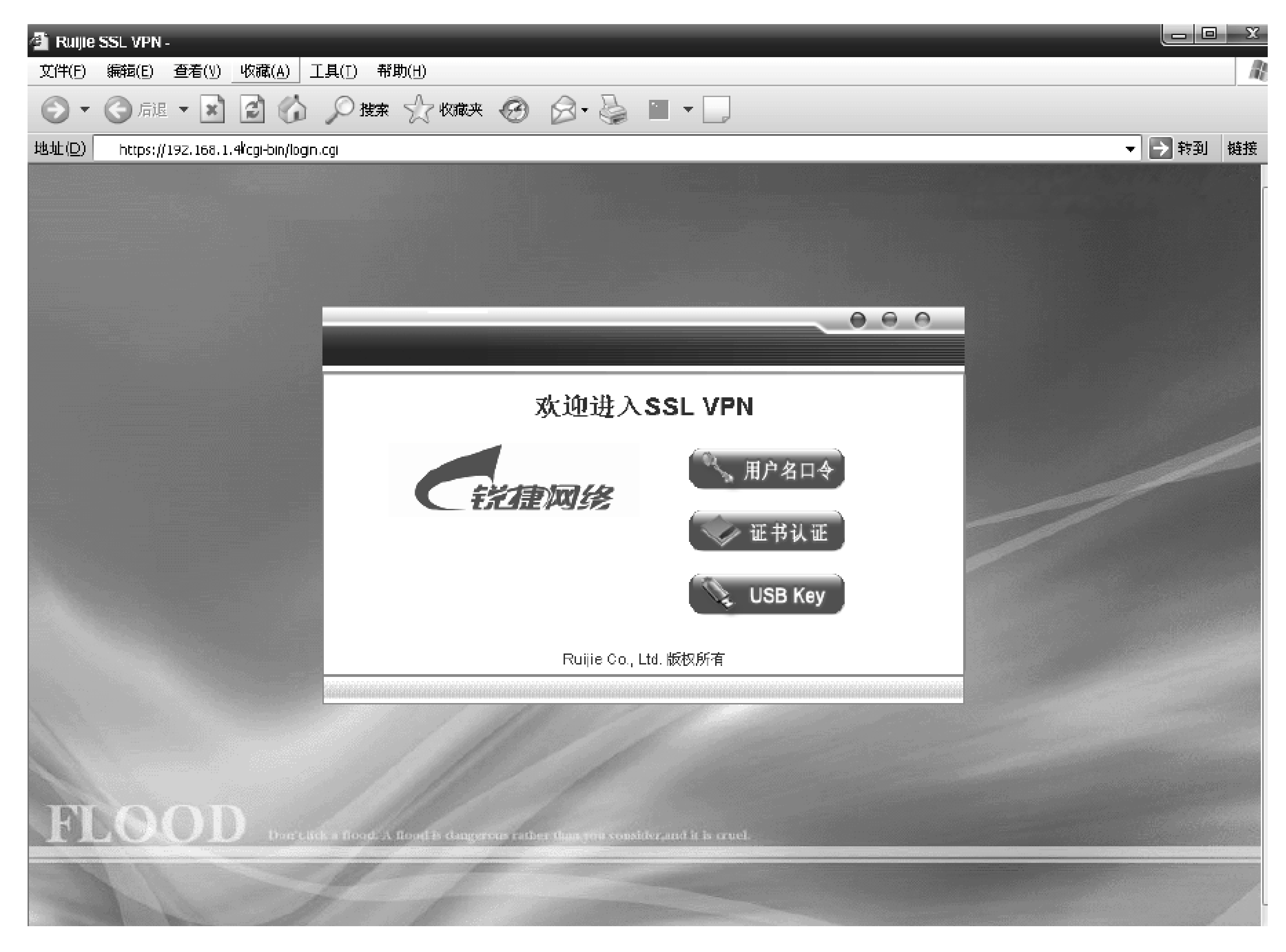


图 4-142　安装插件与 SSL VPN 客户端程序



图 4-143　输入用户名口令及验证码

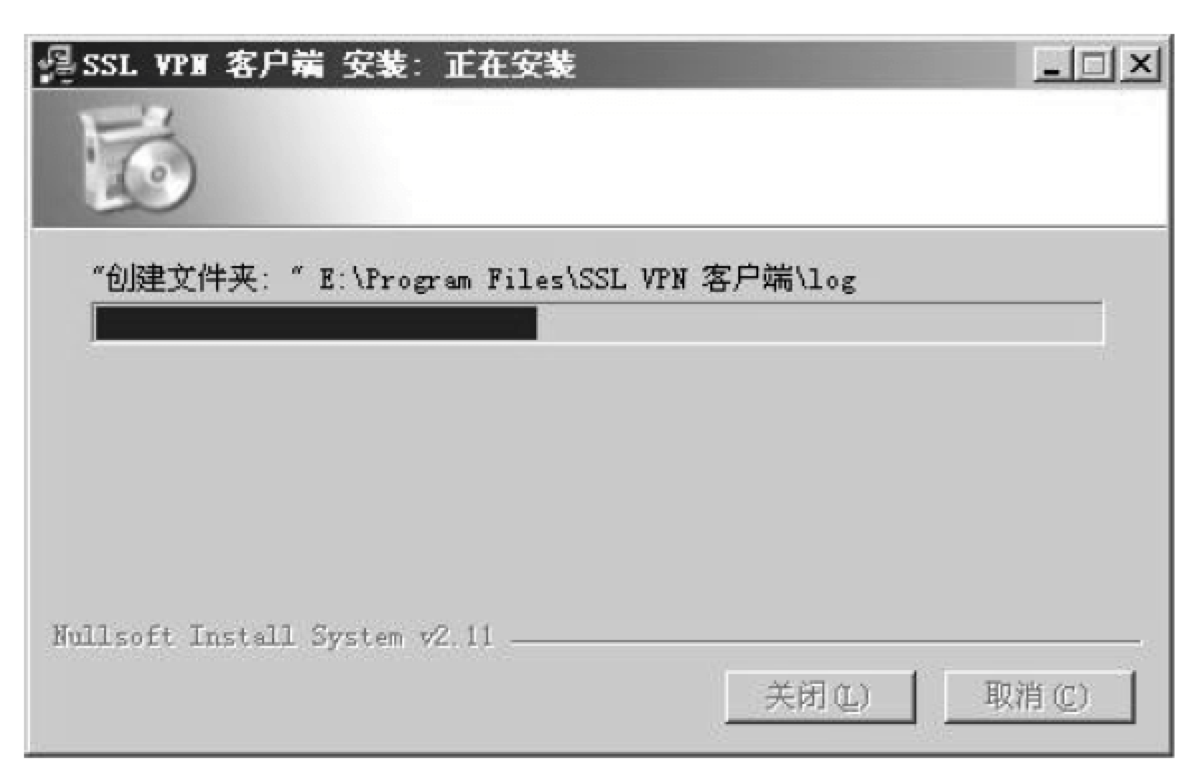


图 4-144　安装插件和 SSL VPN 客户端

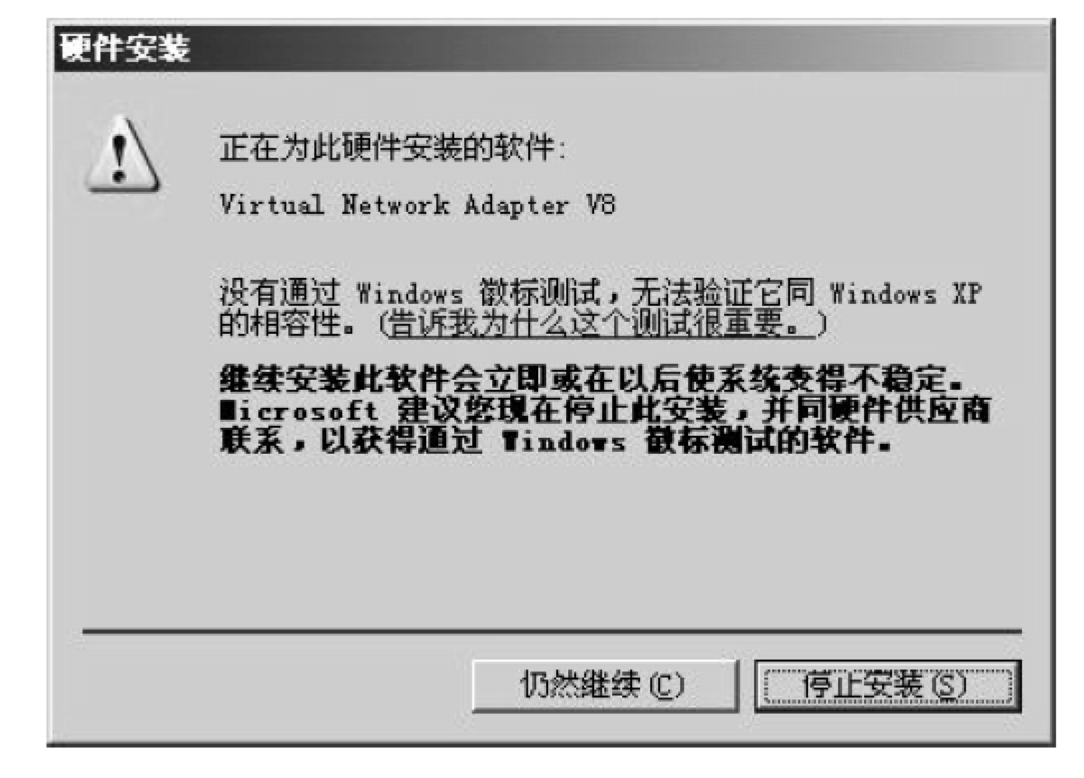


图 4-145　完成 SSL VPN 客户端的安装

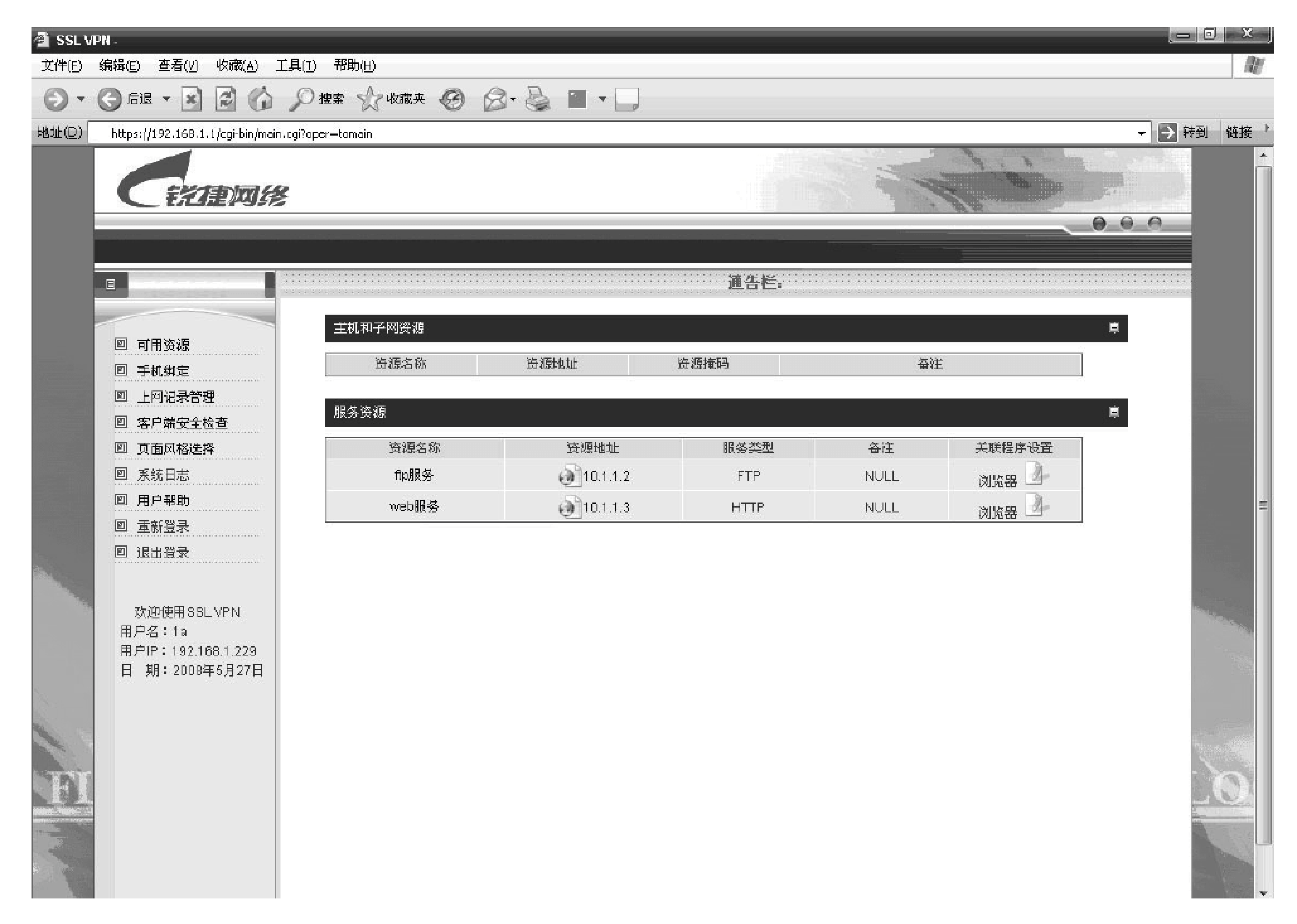


图 4-146 能够访问的服务器资源



图 4-147 FTP 服务资源的访问

或者在 Windows 系统 PC 上打开 FlashFXP 工具,访问 10.1.1.2,即可对内网 FTP 服务器进行下载、上传、删除等操作,如图 4-148 所示。

(4) 内网 Web 服务资源的访问。

直接单击浏览器的服务资源列表中的“Web 服务资源”,即可访问内网 Web 服务资源 10.1.1.3,如图 4-149 所示。

(5) 内网远程桌面管理服务资源的访问。

在 Windows 系统 PC 上的远程桌面连接程序,在计算机栏中输入 10.1.1.4,单击“连接”按钮。

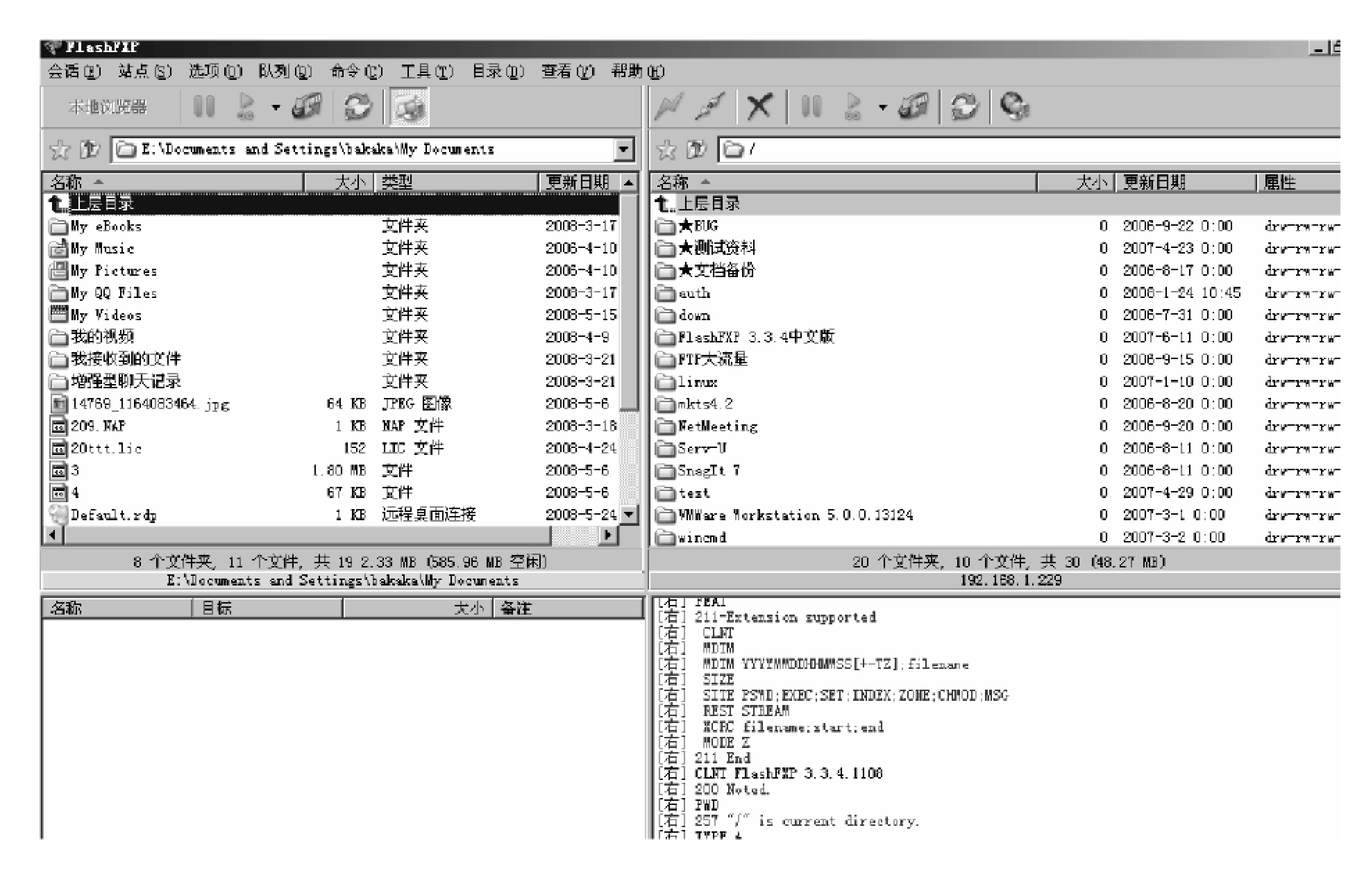


图 4-148　使用 FlashFXP 对 FTP 服务资源的访问



图 4-149　Web 服务资源的访问

附录 A VPN 技术基础

V——Virtual：虚拟的，不用真正的铺设线路；

P——Private：私有的，安全；

N——Network：网络的，互连互通。

顾名思义，VPN 即虚拟专有网络。它不是真正的物理线路，但能够实现专有网络功能。这里说的虚拟专有网络 VPN 技术，就是利用 Internet 技术来组建企业自己的专有网络，实现异地组网，本地通信效果。VPN 利用隧道加密技术，利用公用网络上建立专用的数据通信网络，实现企事业单位任何两个授权端点间的连接。

虚拟专有网络解决了传统专网组建中需要的费时、费钱、端对端的物理链接，而是利用 Internet 公网的物理链路资源，动态组成，使用户实现"不花钱的专网"效果。用户只需购买 VPN 设备和软件产品，向企业所在地的网络服务提供商支付一定 Internet 接入费用，节约租用专线的费用，即可实现不同地域的客户联系，还大大节省长途通信费用。

通俗地讲，有一家公司北京有一个总部，总部设有多台应用服务器，上海有一个分公司，企业内部的局域网通过 Internet 网，使用 VPN 技术在 Internet 公网上为各分部之间建立一条虚拟通信通道，在上海分部局域网中的用户，可以通过本地计算机上"网上邻居"直接访问北京总部服务器，感觉在本地局域网中的用户一样访问远程网络，如图 A-1 所示。

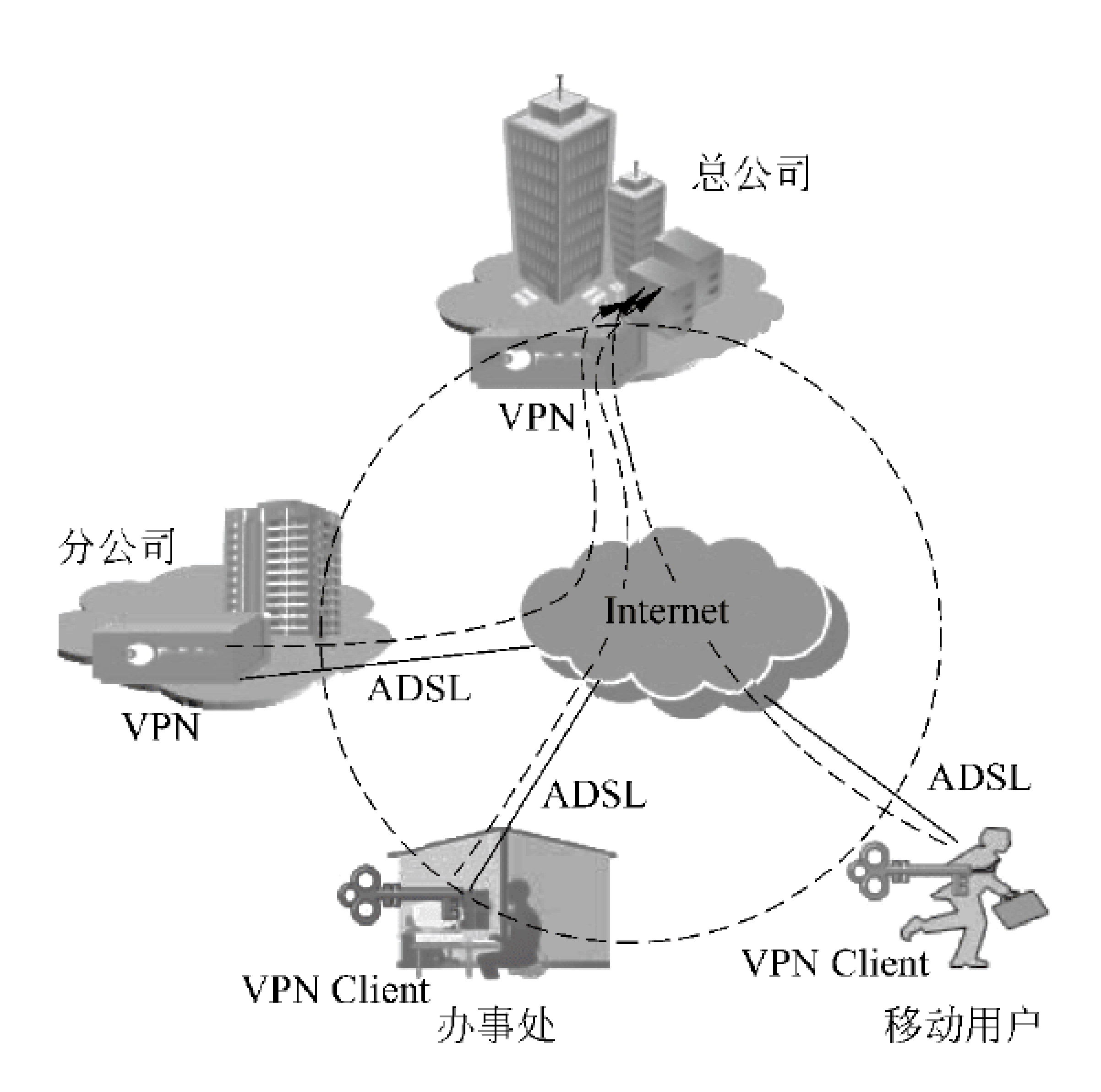


图 A-1 VPN 接入技术和设备在生活中发生场景

通常 VPN 是对企业内部网的扩展，当移动用户或远程网络用户通过拨号方式远程访问企业内部网络时，采用传统的远程访问方式不但通信费用比较高，而且在与内部专用网络中的计算机进行数据传输时，不能保证通信的安全性。为了避免以上问题，通过在企业内部网络之间建立 VPN 连接是一个理想的选择。VPN 虚拟专用网替代了传统的拨号访问，利用 Internet 公网资源作为企业专网的延续，节省昂贵的长途费用，保证了网络安全。

A.1　VPN 概述

虚拟专用网不是真正的专用网络，却能够实现专用网络的功能。VPN 虚拟专网技术在 Internet 公共网络中建立私有专用网络，企业内部保密的数据通过安全的“加密管道”，在公共 Internet 网络中传输，如图 A-2 所示。

Internet 所具备的高带宽、低费用以及无限连接特性，对企业具有极大的诱惑性。但 Internet 网络具有的开放性和松散管理特征，也使企业网络面临的网络安全问题益发尖锐，此问题成了 Internet 作为商务网络必须跨越的重大障碍。而虚拟专用网 VPN 技术，具有防止数据在 Internet 公网传输中被窃听、防止数据在公网传输中被篡改、可以验证数据的真实来源、成本低廉(相对于专线、长途拨号)、应用灵活、可扩展性好等多项特性，是目前和今后一段时间内，企业架构在公司 Internet 上，构建企业内部网络的发展趋势，逐步实现企业网络跨地域安全互联的主要技术。

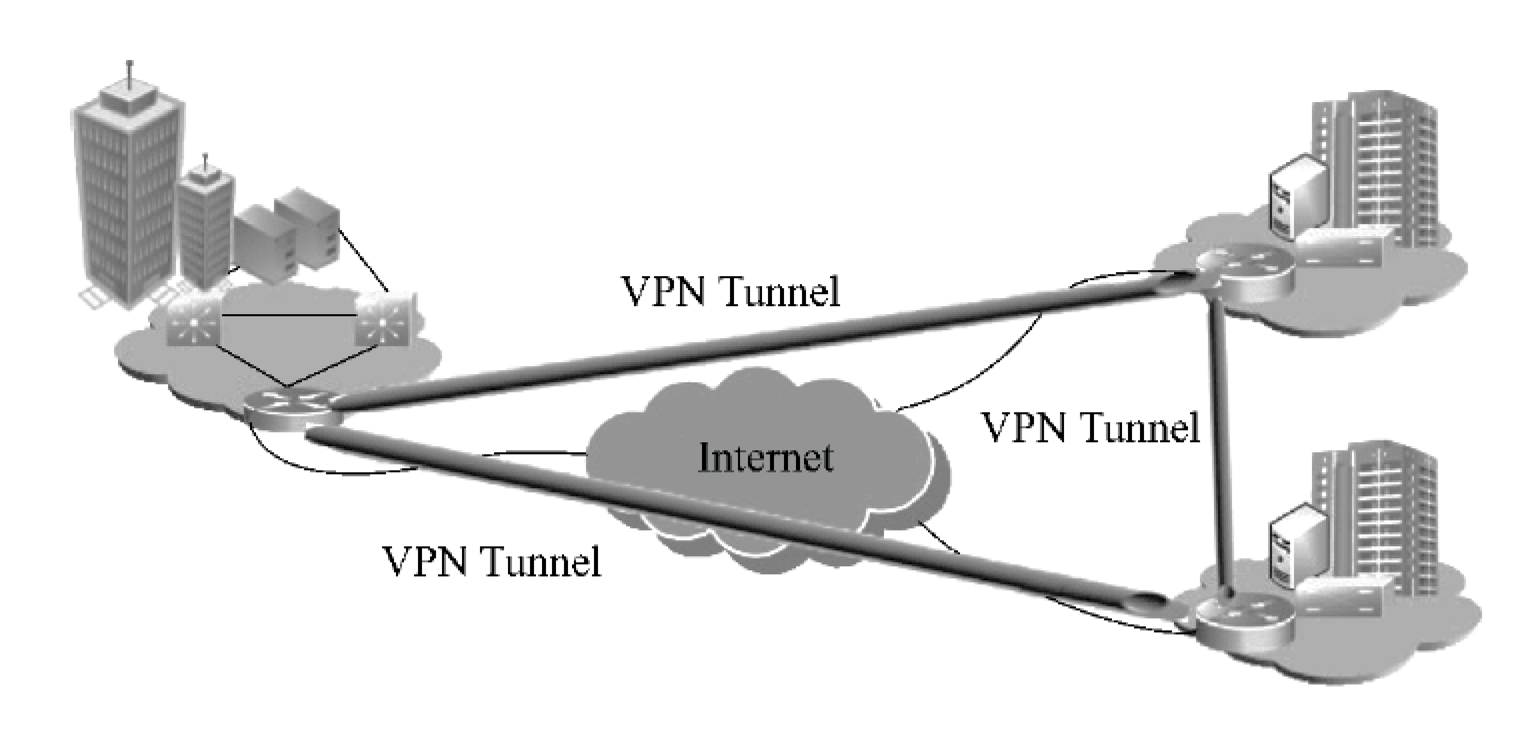


图 A-2　VPN 在 Internet 公众数据网络上的加密管道

IETF 草案理解基于 IP 的 VPN 技术为：“使用 IP 机制，仿真出一个私有的广域网。”VPN 通过私有的隧道技术，在公共数据网络上仿真一条点到点的专线技术。虚拟专用网 VPN 中的数据通过安全“加密管道”在公共网络中传播，企业只需要租用本地的数据专线或者用户通过拨号方式，连接上本地的公共信息网，就可以通过公网互相传递信息，实现分散地点间的企业内部用户，安全连接入企业网中，从而达到安全的数据传输的目的。

VPN 虚拟专用网技术的出现，使企业不再依赖于昂贵的长途拨号以及长途专线服务，而代之以本地 ISP 提供的 VPN 服务。从企业中心站点铺设至当地 ISP 专线，要比传统 WAN 解决方案中长途专线距离短得多，成本也低廉得多。有了 VPN 技术，用户在家里或在出差路途中，就可以利用 Internet 公共网络，对企业内部服务器进行远程安全访

问。VPN 虚拟专用网通过安全的数据通道，将远程用户、公司分支企业、公司业务伙伴等跟公司的企业网连接起来，构成一个扩展的企业网。通过该网络通信本地或远程网络的主机将不会觉察到公共网络的存在，仿佛所有的主机都处于一个网络之中。公共网络仿佛只由本网络独占使用，而事实上并非如此，所以称之为虚拟专用网。

从用户的角度来看，VPN 就是在用户计算机（VPN 客户机）和企业服务器（VPN 服务器）之间建立的点到点的连接，由于数据通过一条仿真专线传输，用户感觉不到公共网络的实际存在，能够像在专线上一样处理企业内部信息。VPN 虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。一个企业的虚拟专用网解决方案，通过将数据流转移到低成本的网络上，将大幅度地减少用户花费在城域网和远程网络连接上的费用。同时，还将简化网络的设计和管理，如图 A-3 所示。

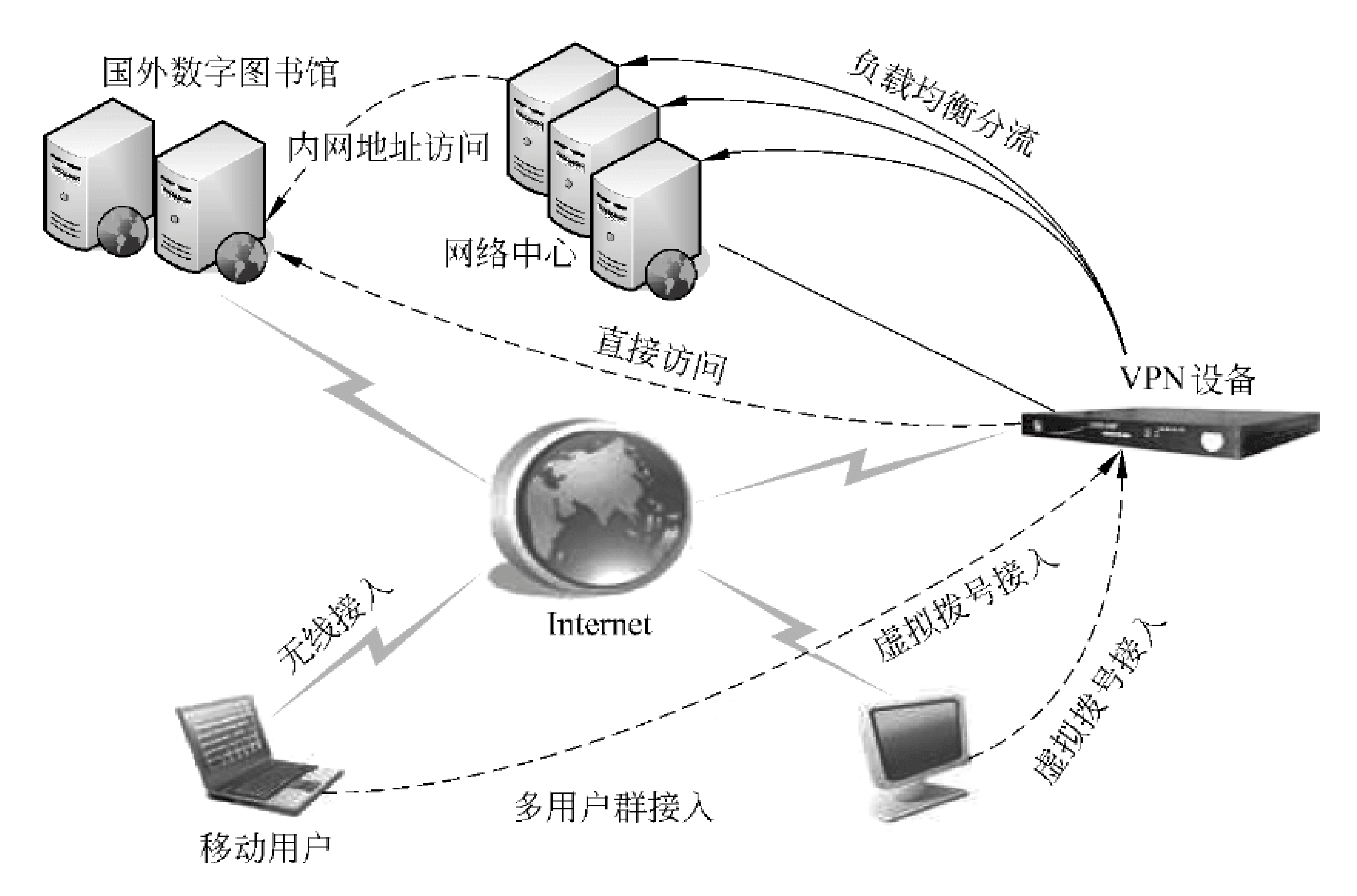


图 A-3 VPN 在用户计算机和企业服务器之间点到点连接

另外虚拟专用网还可以保护用户现有的网络投资。随着用户的商业服务不断发展，企业的虚拟专用网解决方案可以使用户将精力集中到自己的生意上。虚拟专用网还可用于不断增长的移动用户的全球 Internet 接入，以实现安全连接。用于企业网站之间安全通信的内部虚拟专用线路，以及用于连接到商业伙伴和用户的外联虚拟专用网，广泛应用于各个领域，使企业通过公共网络 Internet 实现公司总部和各远程分部，以及在客户之间建立快捷、安全、可靠的通信。

在满足基本应用要求后，有三类用户比较适合采用 VPN。

（1）位置众多，特别是单个用户和远程办公室站点多，例如企业用户、远程教育用户；

（2）用户/站点分布范围广，彼此之间的距离远，遍布全球各地，需通过长途电信，甚至国际长途手段联系的用户；

（3）带宽和时延要求相对适中；对线路保密性和可用性有一定要求的用户。

A.2　VPN 功能和作用

企业中的信息通过 Internet 公网实现跨地域的互联，必然面临 Internet 公网安全问题，由于 Internet 的开放性特征，使用 Internet 公用网络会导致企业间的传输信息容易被窃取，同时攻击者也有可能通过 Internet 公网对企业的内部网络实施攻击，因此需要在企业网之间建立安全的数据专用通道，该通道应具备以下基本安全要素：保证数据真实性；保证数据完整性；保证数据的机密性；提供动态密钥交换功能和集中安全管理服务；提供安全防护措施和访问控制等。

VPN 虚拟专用网技术能有效地解决这些安全问题，在企业网中建立 VPN 虚拟专用网有以下几方面优点。

1. 降低成本

通过公用网来建立 VPN 虚拟专用网通信，与租用 DDN、PSTN 等其他专线方式相比，可以节省大量的费用开支。VPN 技术的最大吸引力是价格，据估算，如果企业放弃租用 DDN 专线而采用 VPN 虚拟专网技术，其整个网络的成本可节约 21％～45％。至于以电话拨号方式接入网络实现数据通信公司，采用 VPN 虚拟专网则可以节约通信成本 50％～80％。

这是由于 VPN 虚拟专网是在 Internet 上临时建立的安全虚拟专用网络，用户节省了永久租用专线的费用。在运行的资金支出上，除了购买 VPN 设备，企业所付出的仅仅是向企业所在地的 ISP 服务商支付一定的上网费用，节省了长途电话费，故 VPN 通信价格更低廉。

2. 容易扩展

如果用户想扩大 VPN 的容量和覆盖范围，只需改变一些配置，或增加几台设备、扩大服务范围；在远程办公室安装 VPN 更简单，只需进行适当的设备配置即可；欲需要增加单机客户端用户，只需在客户端机器上进行简单配置。

3. 伸缩性强

用户如果想与合作伙伴联网，如果没有 VPN，为保证通信的安全，双方的信息技术部门就必须协商如何在双方之间建立租用线路。有了 VPN 虚拟专网技术之后，只需双方配置安全连接信息即可；当不再需要联网时，也可很方便拆除虚拟专网连接。

4. 完全控制主动

企业可以利用公网或在网络内部自己组建管理 VPN 虚拟专网，由企业自己负责来访用户的查验、访问权、网络地址配置、安全性和网络变化管理等重要工作。

5. 全方位安全保护

由于是架构在开放的 Internet 公网上，组建 VPN 企业虚拟专网肯定没有实际组建专线安全，不过通过相关技术（如 IPSec 协议），可以保证虚拟专网足够安全。VPN 虚拟专

网不仅能在网络与网络之间建立专用通道,保护网关与网关之间信息传输安全,而且能在企业内部的用户与网关之间、移动办公用户和网关之间、用户与用户之间建立虚拟的安全通道,实施全方位的安全保护,保证网络的安全。

6. 性价比高

VPN 虚拟专网致力于为企业网络提供整体的安全性,是性能、价格比较高的安全方式,使用简单,管理方便,VPN 虚拟专网产品可以在网络连接中透明地配置,而不需要修改网络或客户端的配置,使用非常方便。此外 VPN 安全产品还可以实现集中管理,即在一点实现对多点 VPN 的配置、监控和维护等。

A.3 VPN 产品体系

VPN 安全产品专用于使用 TCP/IP 体系构建的网络,在网络层提供数据的鉴别、访问控制、隧道传输和加密功能,适用于企业级用户通过公网构建自主、安全、虚拟专网。VPN 产品保证企业内部信息系统之间的各种业务数据安全、透明地通过公共通信环境,是信息系统安全保障体系的基础平台和重要组成部分。有很多可选的 VPN 虚拟专网产品:独立于操作系统的黑匣 VPN,基于路由器的 VPN,基于防火墙的 VPN,还有基于软件的 VPN。

下面就几种常见 VPN 安全产品分别进行介绍。

1. 网络服务商提供的硬件平台 VPN

这是公司与 Internet 连网并享受 VPN 虚拟专网提供服务最简单、最有效的方法。网络服务供应商在公司现场放置一台 VPN 虚拟专网设备,通过配置该设备创建 VPN 隧道,从而实现安全通信。因其方便安装,便于维护和管理,受到国内企事业单位用户的广泛推崇。

使用专用硬件平台的 VPN 设备可以满足企业级用户对数据安全及通信性能的需求,尤其适用于需要进行数据加密及对数据乱码的处理等,对设备的 CPU 处理能力需求很高的环境中。提供这些平台的硬件厂商比较多,比较有名的如国外的 Nortel、Cisco、3Com 等,国内如华为、锐捷、联想等。

组建这类 VPN 平台,虽然投资了大量的硬件设备,但是它具有先天的不足,就是成本太高,对于中、小型企业很难承受。并且由于全是由硬件构成的平台,因此在管理的灵活性和可管理性方面就显得不尽如人意。通常对于专业的 VPN 网络服务提供商来说,选择这一平台较为合适,因为它们有这方面的人才和资金优势。不过现在的主流 VPN 硬件设备制造商都能提供相应的管理软件来支持使用的易用性,如图 A-4 所示。

2. 辅助硬件平台 VPN

这类 VPN 的平台介于软件平台和硬件平台之间,辅助硬件平台的 VPN 主要是指以现有网络设备为基础,再增添适当的 VPN 软件实现 VPN 的功能。这也是一种常见的 VPN 平台,性能也是最好的一种。但是通常这种平台中的硬件也不能完全由原来的网络



图 A-4　硬件平台 VPN

硬件来完成，必要时还得添加专业的 VPN 设备，如 VPN 交换机、VPN 网关或路由器等。这种平台既具备了硬件平台的高性能、高安全性，同时也具有软件平台的灵活性，并且可以利用绝大多数现有硬件设备，节省了总体投资。

3. 基于防火墙 VPN

基于防火墙的 VPN 虚拟专网产品，也是组建 VPN 虚拟专网较常见的一种实现方式，许多厂商都提供这种配置方案。与别的 VPN 相比，基于防火墙的 VPN 虚拟专网并不是一种全新的产品，只是在现有防火墙产品的基础上再增加新功能而已。如今很难找到一个连接 Internet 而不使用防火墙的企业网络。因为这些企业网络已经连到 Internet 网上，所需要的只是增加加密软件，如图 A-5 所示。



图 A-5　新一代防火墙/VPN 网关

基于防火墙的 VPN 虚拟专网建设方案时，有很多厂商的产品可供选择。需要考虑的是所选产品和下层操作系统的关系：防火墙在什么平台上运行？是基于 UNIX、Windows NT，还是别的平台？该操作系统潜在的威胁是什么？因此，如果在防火墙设备上建构 VPN 虚拟专网方案，需要确认底层的操作系统的安全性。当然因防火墙的价格偏高，所以对于某些中小企业用户来说，仍需慎重选择考虑。

4. 基于黑匣的 VPN

在黑匣 VPN 虚拟专网建设方案中，厂商只提供一个黑匣，这里的黑匣是一种安装了加密软件 VPN 隧道的设备。一些黑匣附带有运行于台式机帮助管理的软件，而另一些可以通过 Web 浏览器方式进行配置。这些通过硬件技术的加密设备，比使用软件加密的设备工作起来速度更快。基于黑匣的 VPN 产品可以建立所需的加速隧道，能够更快地执行传输中数据的加密进程。但需要注意的是，并非所有的黑匣 VPN 产品都提供集中管理功能，通常有些也不支持自身记录，需要把一些记录数据发送到另一个数据库进行查询。

5. 基于软件平台的 VPN

当对数据连接速率较低要求不高，对性能和安全性要求不强时，可以利用一些软件公司所提供的完全基于软件 VPN 的产品来实现简单的 VPN 的功能，如 Checkpoint Software 和 Aventail Corp. 等公司的产品。甚至可以不需要另外购置软件，仅依靠微软的 Windows 操作系统，特别是自 Windows 2000 版本以后的系统就可实现纯软件平台的 VPN 连接。

这类 VPN 网络一般性能较差，数据传输速率较低，同时在安全性方面也比较低，一般仅适用于连接用户较少的小型企业。

A.4 VPN 虚拟专网设计

VPN 虚拟专网实际上就是将 Internet 看做一种公有数据网，这种公有网和 PSTN 电话网在数据传输上没有本质的区别。从用户角度来看，数据都被正确传送到目的地。但对企业来说，VPN 是在公共数据网上建立的，用以传输企业内部信息的网络，因此也被称为私有网。

目前共有三种类型的 VPN 虚拟专网，它们分别是远程访问虚拟专网(Access VPN)、企业内部虚拟专网(Intranet VPN)和扩展的企业内部虚拟专网(Extranet VPN)，这三种类型的 VPN 分别与构建传统的远程访问网络、企业内部的 Intranet 及企业网和相关合作伙伴的企业网所构成的 Extranet 相对应，用户可以根据自己实际情况进行选择。

1. Access VPN 虚拟专网实现

Access VPN 又称为拨号 VPN (即 VPDN)，是指企业员工或企业的分公司，通过公网远程拨号的方式构筑的 VPN 虚拟网。如果企业的内部人员移动或有远程办公需要，或者商家要提供 B2C 的安全访问服务，就可以考虑使用 Access VPN 虚拟专网。

Access VPN 虚拟专网通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。Access VPN 能使用户随时、随地以其所需的方式访问企业资源。Access VPN 包括能随时使用如模拟拨号 Modem、ISDN、数字用户线路(xDSL)和有线电视电缆等技术，实现安全地连接移动用户、远程工作者或分支企业之间通信。这种方式相对传统的拨号访问具有明显的费用优势，特别对于需要移动办公的企业来说不失为一种经济、安全、灵活自由的网络互联方式，此外这种方式通常也是许多大、中型企业所必需的，如图 A-6 所示。

Access VPN 虚拟专网最适用于公司内部流动人员远程办公情况，出差员工利用当地 ISP 网络接入，使用本机上 VPN 客户端软件，就可以享受 VPN 虚拟专网服务，实现和公司的 VPN 网关建立私有的隧道连接。内网中的 RADIUS 服务器可对员工进行验证和授权，保证连接的安全，同时负担的通信费用也大大降低。

Access VPN 虚拟专网对用户的吸引力在于：减少用于相关的调制解调器和终端服务设备的资金及费用，简化网络安装；实现本地拨号接入的功能就可以取代远距离接入，

这样能显著降低远距离通信的费用;此外具有极大的可扩展性,可以简便地实现对新加入网络中的新用户进行调度;此外还可以实现基于标准远端验证拨入用户服务,基于策略功能的安全服务;将工作重心从管理和保留运作拨号网络的工作人员转到公司的核心业务上来。

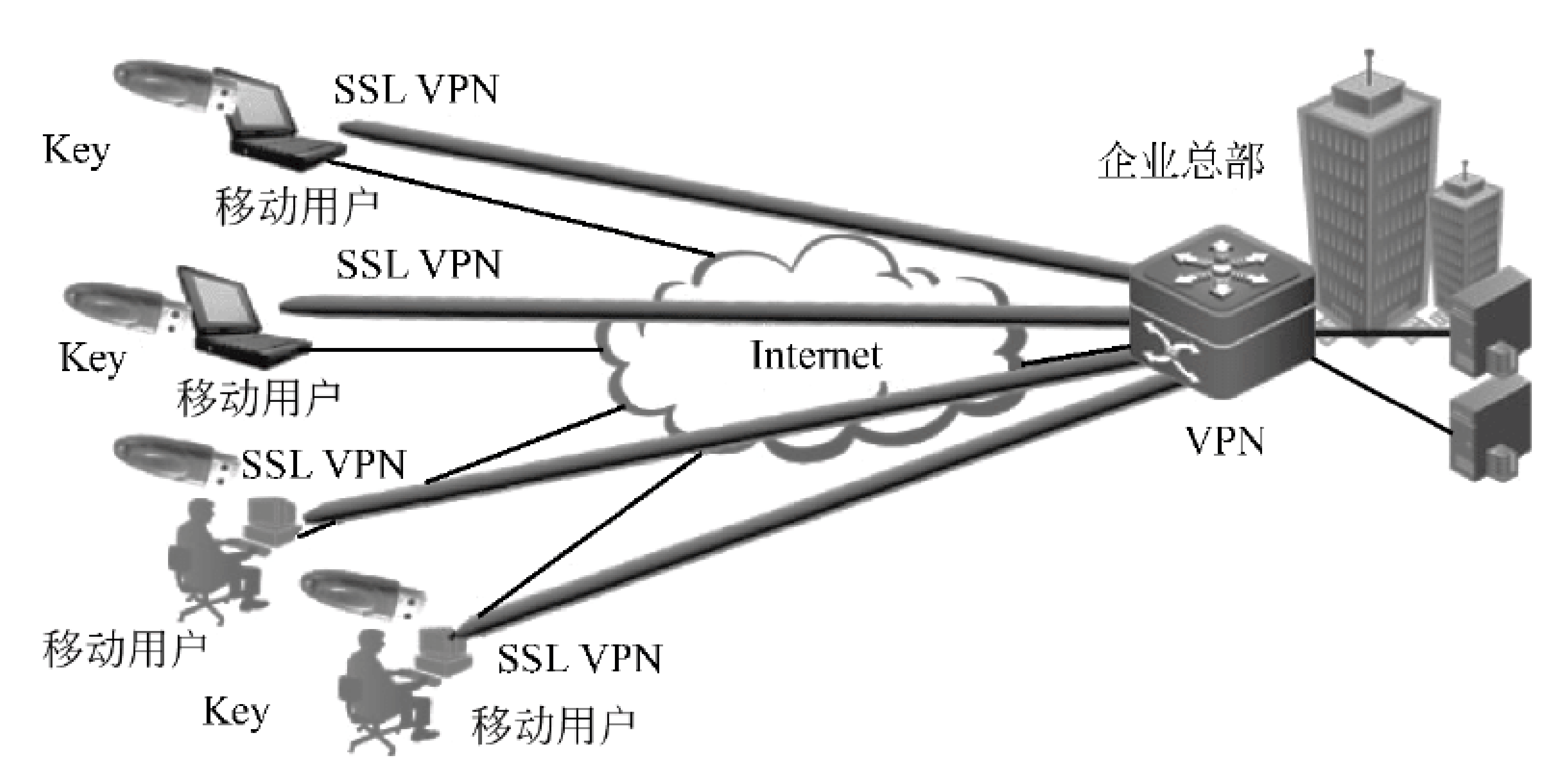


图 A-6　Access VPN 虚拟专网的实现方式

2. Intranet VPN 虚拟专网的实现

如果要进行企业内部各分支企业的互联,使用 Intranet VPN 虚拟专网是很好的方式。

Intranet VPN 即企业的总部与分支企业间通过 VPN 虚拟网进行网络连接技术。如果要进行企业内部各分支企业之间的互联,使用 Intranet VPN 是很好的连接方式。这种 VPN 通过公用因特网或者第三方专用网进行连接,有条件的企业可以采用光纤作为传输介质以提高速度。它的特点就是容易建立连接、连接速度快,最大特点就是它能为各分支企业提供整个 VPN 网络的访问权限。

越来越多的企业需要在全国,乃至世界范围内建立分公司、研究所等,各个分公司之间传统的网络连接方式,一般是租用专线。显然在公司业务增多,公司间通信开展越来越频繁时,网络结构趋于复杂,企业间花费的费用也越来越昂贵。

利用 VPN 虚拟专网特性可以在 Internet 上,组建世界范围内 Intranet VPN 虚拟专网。利用 Internet 线路保证网络互联性,而利用 VPN 的隧道、加密等 VPN 特性,可以保证信息在整个 Intranet VPN 虚拟专网上安全传输。Intranet VPN 虚拟专网通过一个使用专用连接共享基础设施,连接企业总部、远程办事处和分支企业。整个企业专用网络使用相同策略,包括安全服务、质量(QoS)、可管理性和可靠性。

如图 A-7 所示网络环境,显示 Intranet VPN 虚拟专网技术应用的工作场景,它对用户的吸引力在于:减少 WAN 带宽的费用;能使用灵活的拓扑结构,包括全网络连接;新加入的站点能更快、更容易地被接入;通过设备供应商 WAN 的连接冗余,可以延长网络的可用时间。

3. Extranet VPN 虚拟专网的实现

Extranet VPN 是企业间在发生收购、兼并之后或不同的企业间建立战略联盟后,实

现不同企业网通过公网来构筑 VPN 的虚拟网方法。

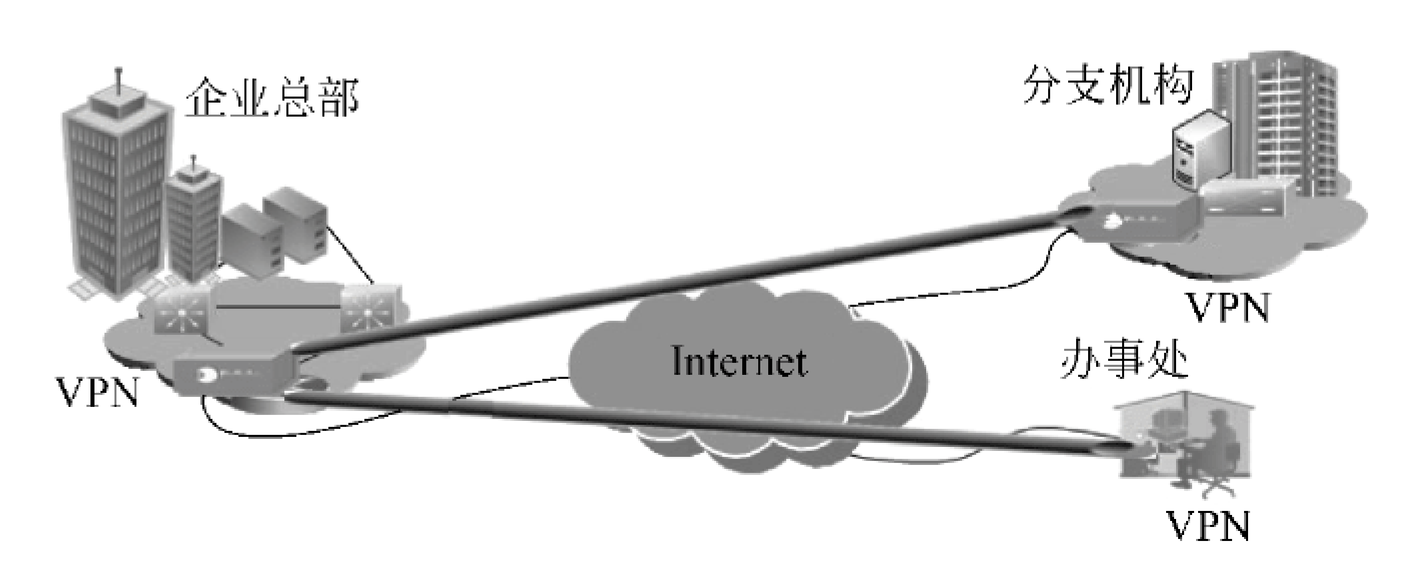


图 A-7　Intranet VPN 虚拟专网的实现方式

随着信息时代的到来,各个企业越来越重视各种信息处理。希望提供给客户最快捷方便信息服务,通过各种方式了解客户需要,同时各个企业之间合作关系也越来越多,信息交换日益频繁。因特网为这一发展趋势提供了良好基础,而如何利用因特网进行安全有效的信息管理,是企业发展中不可避免的一个关键问题,Extranet VPN 为这样的发展趋势提供了安全保障。利用 VPN 技术可以组建企业间安全 Extranet 网,既可以向客户、合作伙伴提供有效信息服务,又可以保证自身内部网络安全。

Extranet VPN 对用户的吸引力在于:能容易地对外部网进行部署和管理,外部网的连接可以使用与内部网和远端访问 VPN 相同的架构和协议进行部署。不同是接入许可区别,外部网的用户被许可只有一次机会连接到其合作的网络,并且只拥有部分网络资源访问权限,这要求企业用户对各外部用户进行相应访问权限的设定。

Extranet VPN 虚拟专网通过使用专用连接,共享基础设施,将客户、供应商、合作伙伴连接到企业内部网。企业拥有与专用网络的相同政策:包括安全服务、质量(QoS)、可管理性和可靠性,如图 A-8 所示网络场景。

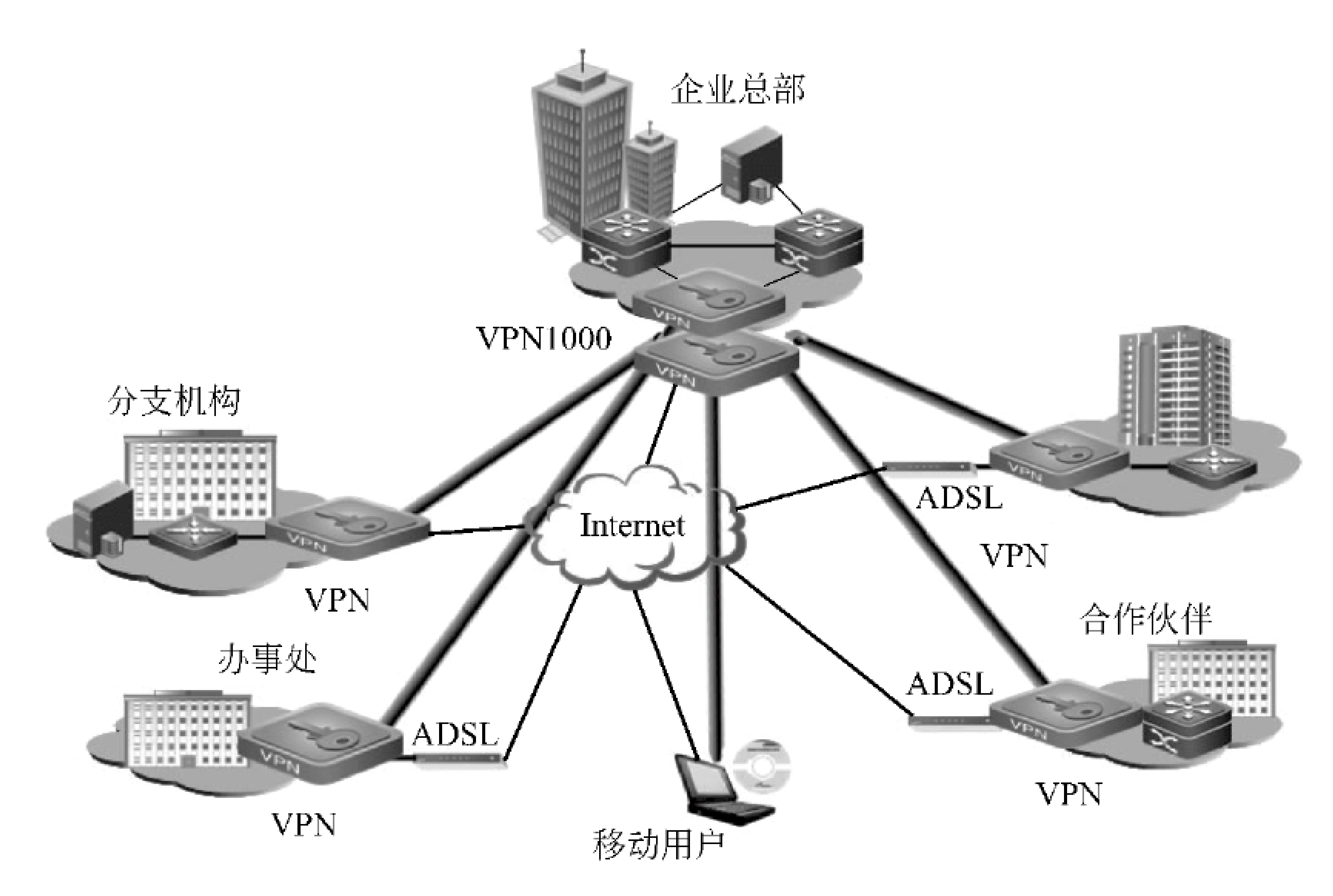


图 A-8　Extranet VPN 虚拟专网的实现方式

A.5 VPN 虚拟专网安全技术

由于企业网络中传输的是私有信息，VPN 虚拟专网中用户对数据的安全性都比较关心，安全问题是 VPN 技术的核心问题。目前组建 VPN 虚拟专网主要采用四项技术来保证安全，这四项技术分别是隧道技术（Tunneling）、加解密技术（Encryption & Decryption）、密钥管理技术（Key Management）、使用者与设备身份认证技术（Authentication），保证企业员工安全访问公司内部网络中资源。

1. 隧道技术

隧道技术是 VPN 虚拟专网的基础技术，类似于点对点连接技术。隧道技术在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道由隧道协议形成，分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包封装入隧道协议中。这种双层封装方法形成的数据包，靠第二层协议进行传输。第二层隧道协议有 L2F、PPTP、L2TP 等。其中 L2TP 协议是目前 IETF 的标准，由 IETF 组织融合 PPTP 协议与 L2F 协议而形成。

第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议在网络上进行传输。第三层隧道协议有 VTP、IPSec 等。其中 IPSec 由一组 RFC 文档组成，定义了一套系统来提供安全协议选择、安全算法，确定服务所使用的密钥等服务，从而在 IP 层提供安全保障。

2 加解密技术

数据加密的基本过程就是对原来明文的文件或数据，按某种算法进行处理，使其成为不可读的一段代码，通常称为“密文”。密文代码只能在输入相应的密钥之后才能显示出来内容。通过这样的途径来达到保护数据不被非法人窃取、阅读的目的。

加解密技术是数据通信中一项较成熟的技术，VPN 可直接利用现有加密技术，如 DES、Triple-DES 等。加密后的数据包即使在传输中被窃取，非法获取者也只能看到一堆乱码，必须拥有相应的密钥（Ericryption key）才能破译。而要破译密钥的话，其所需的设备与时间则需视加密技术及密钥长度而定。如使用 56 位加密的 DES，以现今的普通 PC 计算，需要几十年才能破译；而使用 112 位的 Triple-DES 加密技术目前则被视为不可破译。

加解密技术依密钥可分为两大类：①对称式密码学（Symmetric cryptography），有时又称密钥式密码学（Secret-key crvptography）；②非对称式密码学（Asymmetric crvptography），又称公用钥匙密码学（Public-key cryptography）。另外，还可依保密方式来区分，主要可分为分组密码（Block Cipher）和序列密码（Stream Cipher）。

对称式的加解密技术，或称为专用密钥（也称常规加密），由通信双方共享一个秘密密钥，加密与解密均使用同一把钥匙对称加密。发送方在进行数学运算时使用密钥将明文加密成密文。接受方使用相同的密钥将密文还原成明文。常见加密技术中 RSA RC4 算法、数据加密标准（DES）、国际数据加密算法（IDEA）以及 Skipjack 加密技术都属于对称

加密方式。

非对称加密,或公用密钥,通信双方使用两个不同的密钥,加密与解密使用不同的钥匙。一个是只有发送方知道的专用密钥,另一个则是对应的公用密钥,任何人都可以获得公用密钥。专用密钥和公用密钥在加密算法上相互关联,一个用于数据加密,另一个用于数据解密,公用密钥加密技术允许对信息进行数字签名。

数字签名技术发送一方使用专用密钥对所发送信息的某一部分进行加密。接受方收到该信息后,使用发送方的公用密钥解密数字签名,验证发送方身份。其中加密技术RSA算法被采用最多。由于对称式密码算法的运算速度较非对称式密码演算法快(约100~1000倍),所以现行的VPN设备都采用DES或Triple-DES作为加解密所用的算法。而如果使用对称式加上非对称式的混合(Hybrid)密钥管理功能,进行网络上密钥的交换与管理,不但可提供较快的传输速度,还有更好的保密功能,也更难破解。分组密码算法适合大量数据的传输,通常使用硬件来执行以提高运算效率。

3. 密钥管理技术

如果窃取数据包者不能获得密钥。那只能采用穷举法破译,这在目前加密技术严密情况下几乎不可能。密钥管理技术主要任务是如何在公用数据网上安全地传递密钥而不被窃取。现行密钥管理技术又分为SKIP与ISAKMP/OAKLEY两种:SKIP技术由Sun公司开发,主要是利用Diffie-Hellmail演算法则,在网络上传输密钥的一种技术。而在ISAKMP技术中,双方都有两把密钥,分别用于公用、私用场合。目前ISAKMP/OAKLEY技术逐渐整合于IPv6协议中,成为IPv6的安全标准之一。

在数据加密和密钥管理方面,VPN采用微软的点对点加密算法MPPE协议和网际协议安全IPSec机制,对数据进行加密。并采用公、私密钥对的方法,对密钥进行管理。其中MPPE算法使Windows 95、98、XP和NT 4.0终端,可以在全球任何地方进行安全通信。MPPE加密确保了数据的安全传输,并具有最小的公共密钥开销。以上的身份验证和加密手段,由远程VPN服务器强制执行。对于采用拨号方式建立VPN的连接,VPN连接可以实现双重数据加密,使网络数据传输更安全。

对于企业中敏感的数据,可以使用VPN连接,通过VPN服务器,将高度敏感企业网中的数据服务器物理地进行分隔,只有企业Intranet上拥有适当权限的用户,才能通过远程访问建立与VPN服务器的VPN连接,访问敏感部门网络中受到保护的资源。

4. 使用者与设备身份认证技术

公用网络上有众多的使用者与设备,如何正确地辨认合法的使用者与设备,使只有授权的本单位的人员才能与设备互通,构成一个安全的VPN,并让未授权者无法进入系统,这就是使用者与设备身份确认技术要解决的问题。

辨认合法使用者方法很多,最常使用的是使用者名称与密码或卡片式两段认证方式。设备认证则需依赖由电子证书核发单位(Certificate Authority)颁发X.509电子证书(Certificate)。通信双方将此证书对比后,如果对比正确,双方才开始交换数据。

在用户身份验证安全技术方面,VPN通过使用点到点协议(PPP)用户级身份验证的方法来进行验证,这些验证方法包括密码身份验证协议(PAP)、质询握手身份验证协议

(CHAP)、Shiva 密码身份验证协议(SPAP)、Microsoft 质询握手身份验证协议(MS-CHAP)和可选的可扩展身份验证协议(EAP)。

A.6　VPN 隧道技术

VPN 虚拟专有网络的隧道技术是一种通过 Internet 网络的基础设施，在企业网络之间传递数据的方式。使用隧道技术来传递的数据，可以是不同协议的数据包。隧道协议将这些不同类型协议的数据包，重新封装在新的包头中发送。新的包头提供了路由信息，从而使封装的负载数据能够通过互联网 Internet 传递。被封装的数据包在隧道的两个端点之间通过公共 Internet 网络进行路由。被封装的数据传递时所经过的逻辑路径称为隧道。当数据包到达通信终点后，将被拆封并转发到最终目的地，如图 A-9 所示。

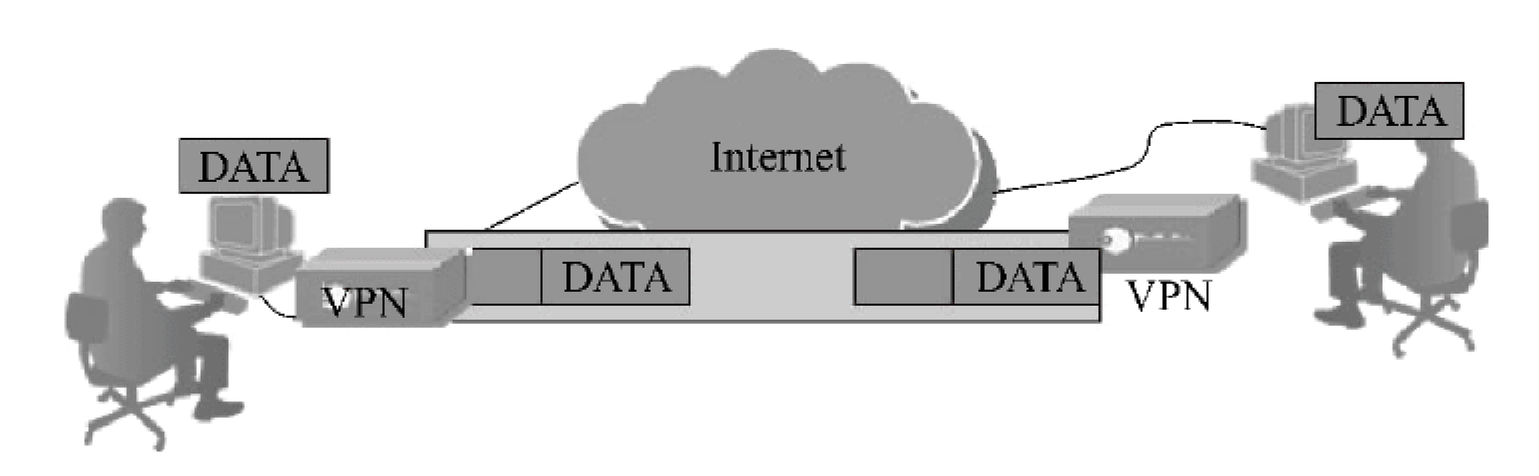


图 A-9　VPN 隧道技术

被封装的数据包在公共 Internet 网络上传递时，所经过的逻辑路径称为隧道。封装的数据包一旦到达目标网络终点，数据将被解包并转发到最终目的计算机。隧道技术是 VPN 虚拟专有网络最重要的技术之一，包括数据封装、数据传输和数据拆封在内几个阶段。VPN 虚拟专有网络的隧道技术，通过公共网络的基础设施，在专用网络或专用设备之间实现加密数据的安全通信，通信的内容可以是任何通信协议的数据包。

在 VPN 隧道中，通信过程能确保通信通道的专用性，并且传输的数据是经过压缩、加密的，所以 VPN 通信同样具有专用网络的通信安全性。

整个 VPN 隧道通信过程可以简化为以下 4 个通用步骤来解释说明。

(1) 客户机向 VPN 服务器发出请求；

(2) VPN 服务器响应请求，并向客户机发出身份质询，客户机将加密的用户身份验证响应信息发送到 VPN 服务器上；

(3) VPN 服务器根据用户数据库检查该响应，如果账户有效，VPN 服务器将检查该用户是否具有远程访问权限；如果该用户拥有远程访问的权限，VPN 服务器接受此连接；

(4) 最后 VPN 服务器将在身份验证过程中产生客户机和服务器公有密钥，用来对数据进行加密，然后通过 VPN 隧道技术进行封装、加密、传输到目的内部网络。

VPN 具体实现是采用隧道技术，将企业网的数据封装在隧道中进行传输。建立 VPN 隧道技术有多种方式，包括 L2TP、IPSec、PPTP、GRE、SSL 等隧道类型，其中 IPSec 协议是 VPN 隧道中安全加密功能最完整的技术之一。VPN 隧道所使用的公共网络，可以是任何类型的通信网络，如 Internet 或 Intranet。为创建隧道，VPN 的客户机和服务器

之间必须使用相同的隧道协议。

按照 OSI 参考模型划分，隧道技术可以分为第二层隧道技术和以第三层隧道技术。它们的本质区别在于用户的数据包被封装在哪种数据包中在隧道中传输。第二层隧道技术对应于 OSI 模型中的数据链路层，使用帧作为数据传输单位，如 PPTP 和 L2TP 隧道协议，将数据封装在点对点协议的帧中通过 Internet 网络发送。第三层隧道协议对应 OSI 模型中的网络层，使用包作为数据传输单位，如安全 IP 隧道模式 IPSec 协议，是将原来数据包封装在附加了 IP 包头的新数据包中通过 Internet 网络传送。

此外 VPN 隧道还可分为自愿隧道（Voluntarytunne）和强制隧道（Compulsorytunnel）两种类型。

自愿隧道是客户端计算机通过发送 VPN 请求，配置和创建一条自愿隧道，此时用户端计算机成为隧道一个端点，是目前最普遍使用的隧道类型。当一台工作站或路由器使用隧道客户软件，创建到目标隧道服务器的虚拟连接时，即可建立自愿隧道。为实现这一目的，客户端计算机必须安装适当隧道协议。自愿隧道需要有一条 IP 连接（通过局域网或拨号线路），客户端必须在建立隧道之前创建与公共网络的连接。典型的例子是因特网拨号用户，必须在创建因特网自愿隧道之前，拨通本地 ISP 取得与因特网的连接。

通过支持 VPN 而接入服务器配置和创建一条强制隧道。此时用户端计算机不作为隧道端点，而由客户计算机和隧道服务器之间的远程接入服务器作为隧道客户端，成为隧道的一个端点。目前一些商家提供能够代替客户拨号创建隧道接入服务器，成为客户端计算机提供建立隧道网络设备。强制隧道提供设备包括支持 PPTP 协议的前端处理器（FEP），支持 L2TP 协议的 L2TP 接入集线器（LAC）或支持 IPSec 的安全 IP 网管。

以因特网为例，客户机向位于本地 ISP 能够提供隧道技术的 NAS（网络访问服务器）发出拨号呼叫，ISP 为企业在全国范围内设置一套 FEP。这些 FEP 通过因特网创建一条到隧道服务器的隧道，隧道服务器与企业的专用网络相连。这样就可以将不同地方合并成企业网络端一条单一的因特网连接。因为客户只能使用由 FEP 创建的隧道，所以称为强制隧道。一旦最初的连接成功，所有客户端的数据流将自动通过隧道发送。使用强制隧道，客户端计算机建立单一的 PPP 连接，当客户拨入 NAS 时，一条隧道将被创建，所有的数据流自动通过该隧道路由。可以配置 FEP 为所有的拨号客户，创建到指定隧道服务器的隧道，也可以配置 FEP 基于不同的用户名或目的地创建不同的隧道。

强制隧道技术为每个客户创建独立的隧道。FEP 和隧道服务器之间建立的隧道可以被多个拨号客户共享，而不必为每个客户建立一条新的隧道。因此，一条隧道中可能会传递多个客户的数据信息，只有在最后一个隧道用户断开连接之后才终止整条隧道。

被封装的数据包在隧道的两个端点之间通过公共互联网络进行路由。被封装数据包在公共互联网络上传递时所经过的逻辑路径称为隧道。一旦到达网络终点，数据将被解包并转发到最终目的地。注意隧道技术是指包括数据封装、传输和解包在内的全过程，如图 A-10 所示。

隧道所使用的传输网络可以是任何类型的公共互联网络，目前主要以普遍使用 Internet。隧道一旦建立，数据就可以通过隧道发送。隧道客户端和服务器使用隧道数据传输协议准备传输数据。例如，当隧道客户端向服务器端发送数据时，客户端首先给负载

数据加上一个隧道数据传送协议包头，然后把封装的数据通过互联网络发送，并由互联网络将数据路由到隧道的服务器端。隧道服务器端收到数据包之后，去除隧道数据传输协议包头，然后将负载数据转发到目标网络。

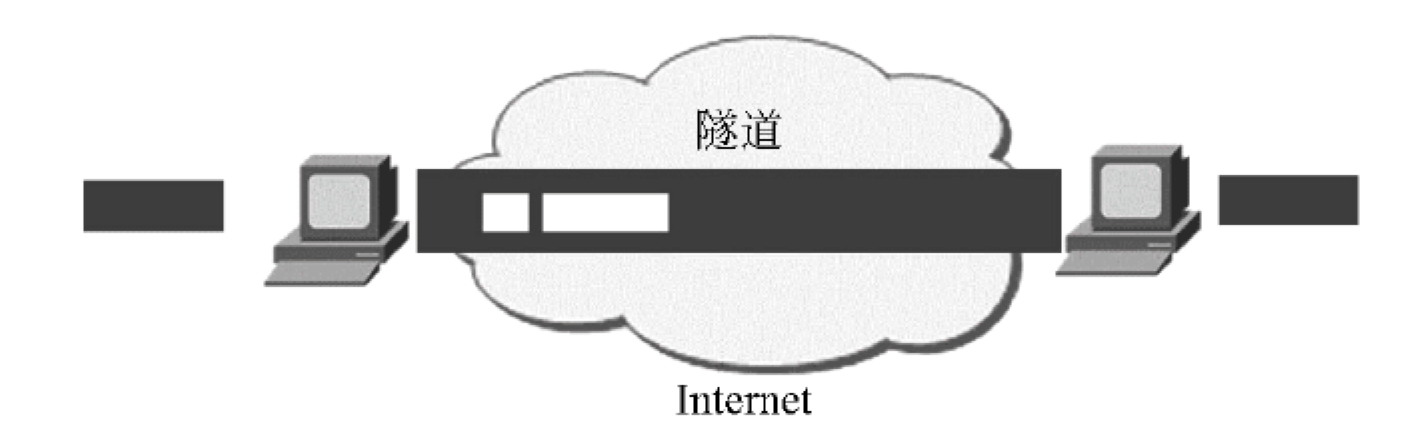


图 A-10　封装的数据包在隧道传输

A.7　VPN 隧道协议

VPN 虚拟专用网的实现依赖于隧道(Tunnel)技术，隧道是一个虚拟的点对点的连接。通过使用互联网络的基础设施，在网络之间传递数据的方式。使用隧道传递的数据可以是不同协议的数据包，隧道协议将这些协议的数据包重新封装在新的包头中发送。新的包头提供了路由信息，从而使封装的数据能够通过互联网络传递。隧道提供一条虚拟通路，使封装的数据包能够在这个通路上传输。为创建传输隧道，隧道两端的客户机和服务器必须使用相同的隧道协议。

目前较为常见的隧道协议大致有两类：第二层隧道协议(包括 PPTP、L2F、L2TP)和第三层隧道协议(包括 IPSec、MPLS、SSL 等)。第二层和第三层隧道协议的区别主要在于：用户数据在网络协议栈的第几层被封装。第二层隧道协议多用于传输第二层网络协议，主要应用于构建远程访问虚拟专网(Access VPN)；第三层隧道协议多用于传输第三层网络协议，主要应用于构建企业内部虚拟专网(Intranet VPN)和扩展的企业内部虚拟专网(Extranet VPN)。

无论哪种隧道协议都是由传输的载体、不同的封装格式以及被传输数据包组成。以第二层隧道协议 L2TP 为例，隧道协议的基本组成如图 A-11 所示。



图 A-11　隧道协议的基本格式

图 A-11 所示隧道协议格式中“传输协议”，主要被用来传送封装协议，IP 是一种常见的传输协议，这是因为 IP 具有强大的路由选择能力，可以运行于不同介质上，且应用最为广泛，此外帧中继、ATM、PVC 和 SVC 也是合适的传输协议。如用户想通过 Internet 将其分公司网络连接起来，网络环境是 IPX，这时用户就可以使用 IP 作为传输协议，通过封装协议封装 IPX 的数据包，就可以在 Internet 网上传送 IPX 数据。

图 A-11 所示隧道协议格式中“封装协议”被用来建立、保持和拆卸隧道，包括 L2F、L2TP、GRE 等协议。而“乘客协议”则是被封装的协议，可以是 PPP、SLIP。

1. PPTP 点对点通道协议

第二层隧道协议点到点隧道协议(Point to Point Tunneling Protocol,PPTP)是点对点的安全隧道协议,为使用电话上网的用户提供安全 VPN 业务,1996 年成为 IETF 草案。PPTP 提供了在 IP 网上建立多协议的安全 VPN 的通信方式,远端用户通过任何支持 PPTP 的 ISP,访问企业的专用网络。PPTP 提供 PPTP 客户机和 PPTP 服务器之间的保密通信。PPTP 客户机是指运行该协议的 PC 机,如启动该协议的 Windows XP。PPTP 服务器是指运行该协议的服务器,如启动该协议的 Windows NT 服务器。

PPTP 可看做是 PPP 协议一种扩展,PPTP 将 PPP 帧封装进 IP 数据包中,通过 Internet 及 Intranet 等发送,提供了一种在 Internet 上建立多协议的安全虚拟专用网的通信方式,远端用户能够通过任何支持 PPTP 的 ISP 服务访问公司专用网络。

如图 A-12 所示 PPTP 点对点通道协议工作场景,Internet 拨号客户首先按常规方式,拨号到 ISP 的接入服务器,建立 PPP 连接。在此基础上客户进行二次拨号,建立到 PPTP 服务器的连接,该连接称为 PPTP 隧道。实质上是基于 IP 协议上的另一个 PPP 连接,其中的 IP 包可以封装多种协议数据,包括 TCP/IP 或 IPX。

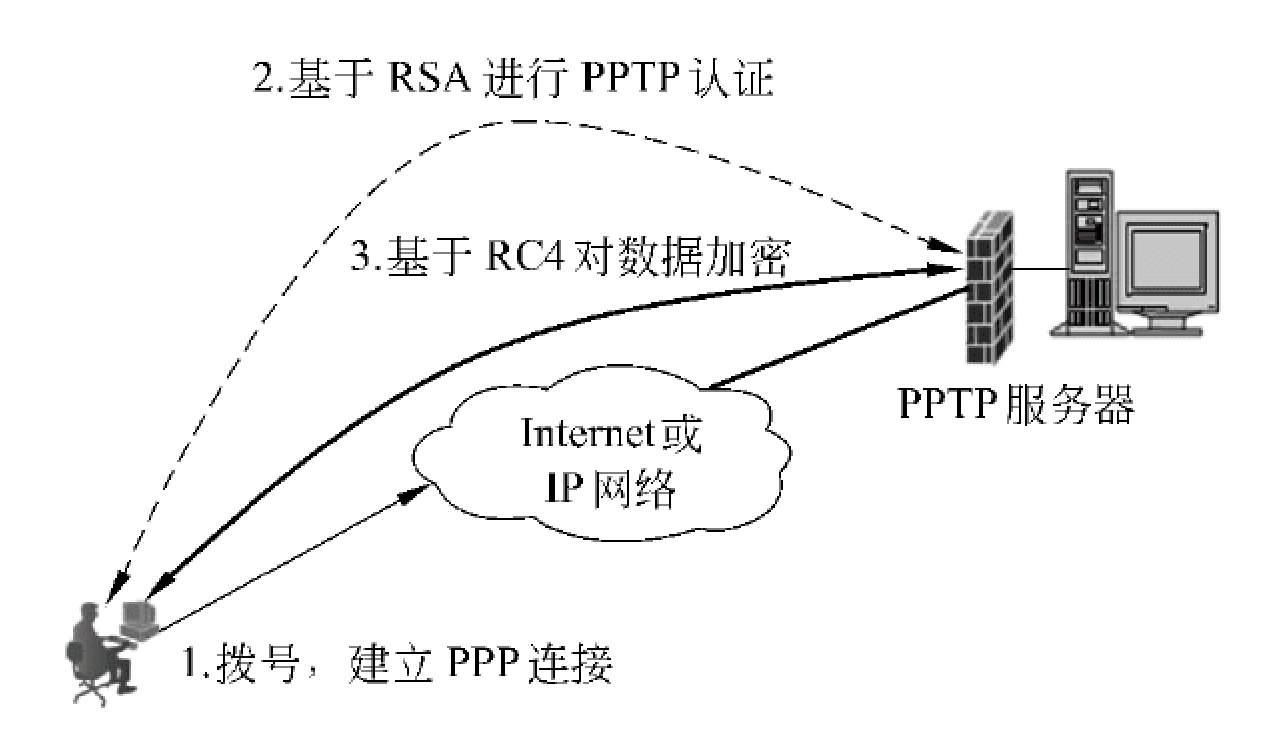


图 A-12 PPTP 点对点通道协议工作过程

PPTP 采用了基于 RSA 公司 RC4 的数据加密方法,保证了虚拟连接通道的安全性。对于直接连到 Internet 上的客户,则不需要第一次 PPP 的拨号连接,可以直接与 PPTP 服务器建立虚拟通道。

PPTP 最大优势是 Microsoft 公司支持,Windows NT4.0 已经包括了 PPTP 客户机和服务器功能。PPTP 另外一个优势是它支持流量控制,可保证客户机与服务器间不拥塞,改善通信性能,最大限度地减少包丢失和重发现象。PPTP 把建立隧道主动权交给了客户,但客户需要在其 PC 上配置 PPTP,这样做既会增加用户的工作量,又会造成网络的安全隐患。另外,PPTP 仅工作于 IP,不具有隧道终点的验证功能,需要依赖用户的验证。

2. L2TP 协议

第二层隧道协议 L2TP(Layer 2 Tunneling Protocol),是一种工业标准的 Internet 隧道协议,功能大致和 PPTP 协议类似,如同样可以对网络数据流进行加密。不过不同之处是,如 PPTP 要求网络为 IP 网络,而 L2TP 则要求面向连接的点对点连接;PPTP 使用单一隧道,L2TP 使用多隧道;L2TP 提供包头压缩、隧道验证,而 PPTP 不支持。

L2TP 从客户端或访问服务器端发起 VPN 连接，把链路层形成的 PPP 帧封装在公共网络（如 IP、ATM、帧中继）中进行隧道传输的封装。L2TP 的好处就在于支持多种协议，用户可以保留原有的 IPX、Appletalk 等协议或原有的 IP 地址，整合多协议服务至现有的因特网服务提供商点。

L2TP 定义了多协议跨越第二层点对点链接的一个封装机制，特别地适用于用户使用众多技术（如拨号 ISDN、ADSL 等），获得第二层连接到网络访问服务器（NAS），如图 A-13 所示。

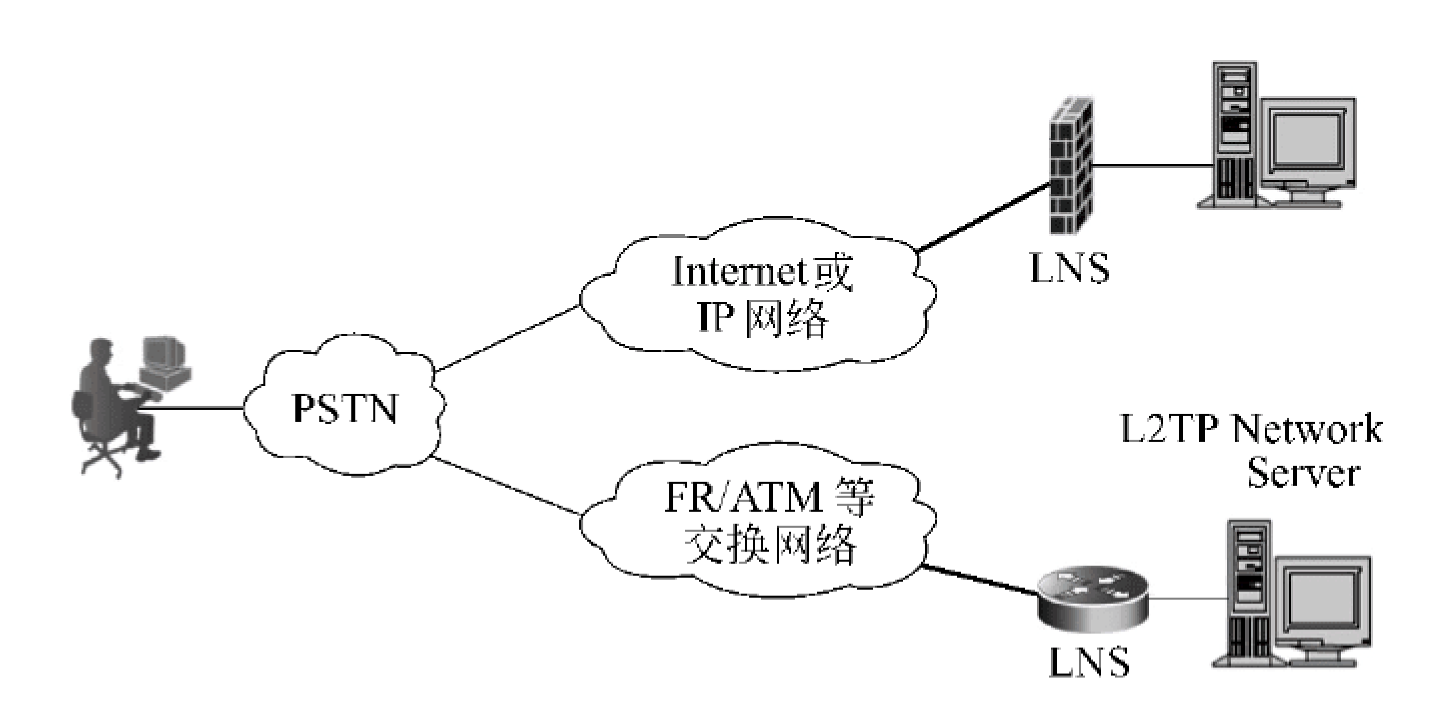


图 A-13　L2TP 协议工作模型

L2TP 还解决了多个 PPP 链路的捆绑问题，PPP 链路捆绑要求其成员均指向同一个 NAS（网络访问服务器），L2TP 可以使物理上连接到不同 NAS 的 PPP 链路，在逻辑上的终结点为同一个物理设备。L2TP 扩展了 PPP 连接，在传统方式中，用户通过模拟电话线或 ISDN/ADSL 与网络访问服务器（NAS）建立一个第二层的连接，并在其上运行 PPP。第二层连接的终结点和 PPP 会话的终结点在同一个设备上（如 NAS），L2TP 作为 PPP 的扩展，提供更强大的功能，包括第二层连接的终结点和 PPP 会话的终结点可以是不同的设备。

L2TP 主要由 LAC（L2TP Access Concentrator）和 LNS（L2TP Network Server）构成。LAC 是支持客户端的 L2TP，用于发起呼叫接收呼叫和建立隧道；LNS 是所有隧道的终点，在传统的 PPP 连接中，用户拨号连接的终点是 LAC，L2TP 使得 PPP 协议的终点延伸到 LNS。

3. IPSec 协议

第二层隧道协议 PPTP、L2TP 等各自有自己的优点，但是都没有很好地解决隧道加密和数据加密的问题。而第三层隧道协议 IPSec 协议则把多种安全技术集合到一起，建立一个安全、可靠的隧道。这些技术包括 Diffie-Hellman 密钥交换技术，DES、RC4、IDEA 数据加密技术，哈希散列算法 HMAC、MD5、SHA、数字签名技术等。

IPSec 协议定义了如何在 IP 数据包中增加字段来加密数据包，以保证 IP 包的完整性、私有性和真实性。使用 IPSec 协议封装的数据在公网上传输，而不必担心数据被监视、修改或伪造，提供了两个主机之间、两个安全网关之间或主机和安全网关主机之间的保护。

自从 1995 年开始 IPSec 的研究工作以来，IETF IPSec 工作组在它的主页上发布了

几十个 Internet 草案文献和 12 个 RFC 文件。第三层隧道协议 IPSec 实际上是一套协议包而不是一个单个的协议，它是一组开放的网络安全协议的总称，其中比较重要的有 RFC2409 IKE 互联网密钥交换、RFC2401 IPSec 协议、RFC2402 AH 验证包头、RFC2406 ESP 加密数据等文件。IPSec 协议族为 VPN 网络提供访问控制、无连接的完整性、数据来源验证、防重放保护、加密以及数据流分类加密等一系列服务。

IPSec 在 IP 层提供安全服务，IPSec 协议的安全结构包括 3 个基本协议：AH 协议＋ESP 协议＋ISAKMP 密钥管理协议。其中报文验证头协议 AH 协议为 IP 包提供信息源验证和完整性保证，主要提供的数据来源验证、数据完整性验证和防报文重放功能；报文安全封装协议 ESP 协议提供加密认证，ESP 在 AH 协议提供安全的功能之外，再提供对 IP 报文的加密功能；密钥管理协议（ISAKMP）提供双方交流时的共享安全信息，如图 A-14 所示。

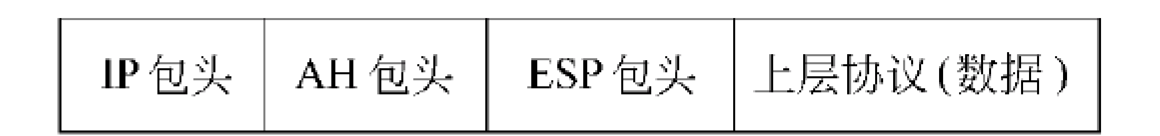


图 A-14 IPSec 协议的安全结构

AH 和 ESP 同时具有认证功能，IPSec 存在两个不同的认证协议，是因为 ESP 要求使用高强度密码学算法，无论实际上是否在使用。而高强度密码学算法在很多国家都存在很严格的政策限制，但认证措施是不受限制，因此 AH 可以在全世界自由使用。另外一个原因是很多情况下人们只使用认证服务。

AH 或 ESP 协议都支持两种模式的使用：隧道模式和传输模式。隧道模式对在不安全的传输链路或 Internet 上，对内部专用 IP 数据包进行加密和封装（此种模式适合于有 NAT 的环境）。传输模式直接对 IP 负载内容（即 TCP 或 UDP 数据）加密（适合于无 NAT 的环境）。

4. SSL VPN

IPSec VPN 是一种比较成熟的 VPN 技术，它能够实现不同子公司与总部的两个不同的局域网远程连接成一个虚拟局域网，从而在广域网间实现以前只有在局域网内，才能实现的安全应用操作，它给当前的企业带来了很多革命性的好处。

当前大多数远程访问解决方案是利用基于第三层隧道协议 IPSec 安全协议模型建立的 VPN 网络。最新的研究表明，近乎 90％的企业利用 VPN 进行内部网和外部网连接，大都只用来进行 WWW 访问和电子邮件通信，另外 10％的用户集中在诸如聊天和其他私有客户端应用。而这些集中在 90％的应用的客户都可以利用一种更简单的 VPN 技术——SSL VPN——来提供更安全、有效的解决方案。基于 SSL 协议的 VPN 远程访问方案，更加容易配置和管理，网络配置成本比 IPSec VPN 也要低很多，所以许多企业开始转向利用基于 SSL 协议的远程访问技术来实现 VPN 通道。

SSL 英文全称是 Secure Sockets Layer，中文名为“安全套接协议层”，它是网景公司提出的基于 Web 应用安全协议。SSL 是一种在 Web 服务协议（HTTP）和 TCP/IP 之间提供数据连接安全的协议，为 TCP/IP 连接提供数据加密，服务器身份验证和消息完整性验证。SSL 被视为因特网上 Web 浏览器和服务器之间实现连接的安全标准。

SSL VPN 通信基于标准 TCP/UDP 协议传输，因而能遍历所有 NAT 设备、基于代理的防火墙和状态检测防火墙。这使得用户能够从任何地方接入，无论是处于其他网络中，还是基于代理的防火墙中，或是宽带网络连接中，而 IPSec VPN 在稍复杂的网络结构中则难以实现，因为它很难实现防火墙和 NAT 遍历，无力解决 IP 地址冲突。相对于传统 IPSec VPN 而言，SSL VPN 似乎正好可以跟它互补。此外 SSL VPN 具有部署简单，无客户端，维护成本低，网络适应强等特点，SSL VPN 能让企业实现更多远程用户在不同地点接入，实现更多网络资源访问，且对客户端设备要求低，因而降低了配置和运行支撑成本。

SSL 安全套接层协议，主要是使用公开密钥体制和 X.509 数字证书技术，保护信息传输的机密性和完整性，它主要适用于点对点之间的信息传输，常用 Web Server 方式。

5. MPLS VPN

多协议标签交换(MPLS)是一种在开放的通信网上，利用标签引导数据高速、高效传输的新技术。这个网络层包转发的新兴标准主要基于互联网工作组(IETF)提交的一系列信令协议，包括标记分配协议(LDP)、资源预留协议(RSVP)和限制路由的标记分配协议(CR-LDP)等。MPLS 是一种可在多种第二层协议上进行标记交换而不用改变现有路由协议的网络技术，将路由与交换合二为一。

多协议标签交换 MPLS 把第三层的智能化、扩展性与第二层交换机制(面向连接的服务除外)结合起来，从而使这种标记交换表现为第三层的交换，却具备第二层的速度。MPLS 能够在一个无连接的网络中引入连接模式的特性，兼容现有的各种主流网络技术，被业界认为是数据网络领域内最有前途的网络解决方案之一。在 IP 网组建中，MPLS 流量技术成为主要的管理网络流量、减少拥塞、保证 IP 网络 QoS 的重要工具。在解决企业网互连，提供各种新业务方面，MPLS VPN 也越来越被运营商看好，成为在 IP 网络运营商提供增值业务的重要手段。

MPLS 实际上就是一种隧道技术，所以使用它来建立 VPN 隧道是十分容易。同时 MPLS 又是一种完备的网络技术，可以用它来建立起 VPN 成员之间简单而高效的 VPN 网络。MPLS VPN 技术适用于实现网络服务质量(QoS)、服务等级划分以及对网络资源的利用率、网络的可靠性等有较高要求的 VPN 业务中。

通常 MPLS 包头的结构如图 A-15 所示，包含 20b 的标签，3b 的 EXP。MPLS 包头的位置介于第二层和第三层之间，俗称 2.5 层，可以承载的报文通常是 IP 包(当然也可以改进，直接承载以太包、ATM 的 AAL5 包甚至 ATM 信元等)。可以承载 MPLS 二层协议可以是 PPP、以太网、ATM 和帧中继等。

对于 PPP 或以太网二层封装，MPLS 包头结构如图 A-20 所示，但是对于 ATM 或帧中继，MPLS 则直接采用分别采用 VPI/VCI 或 DLCI 作为转发的标签。

多协议标签交换(MPLS)是时下最热门的技术之一，它将灵活的三层 IP 选路和高速的二层交换技术完美地结合起来，从而弥补了传统 IP 网络的许多缺陷。它引入了新的标签结构，对 IP 网络的改变较大，引入了“显示路由”机制，为 QoS 提供了更为可靠的保证。

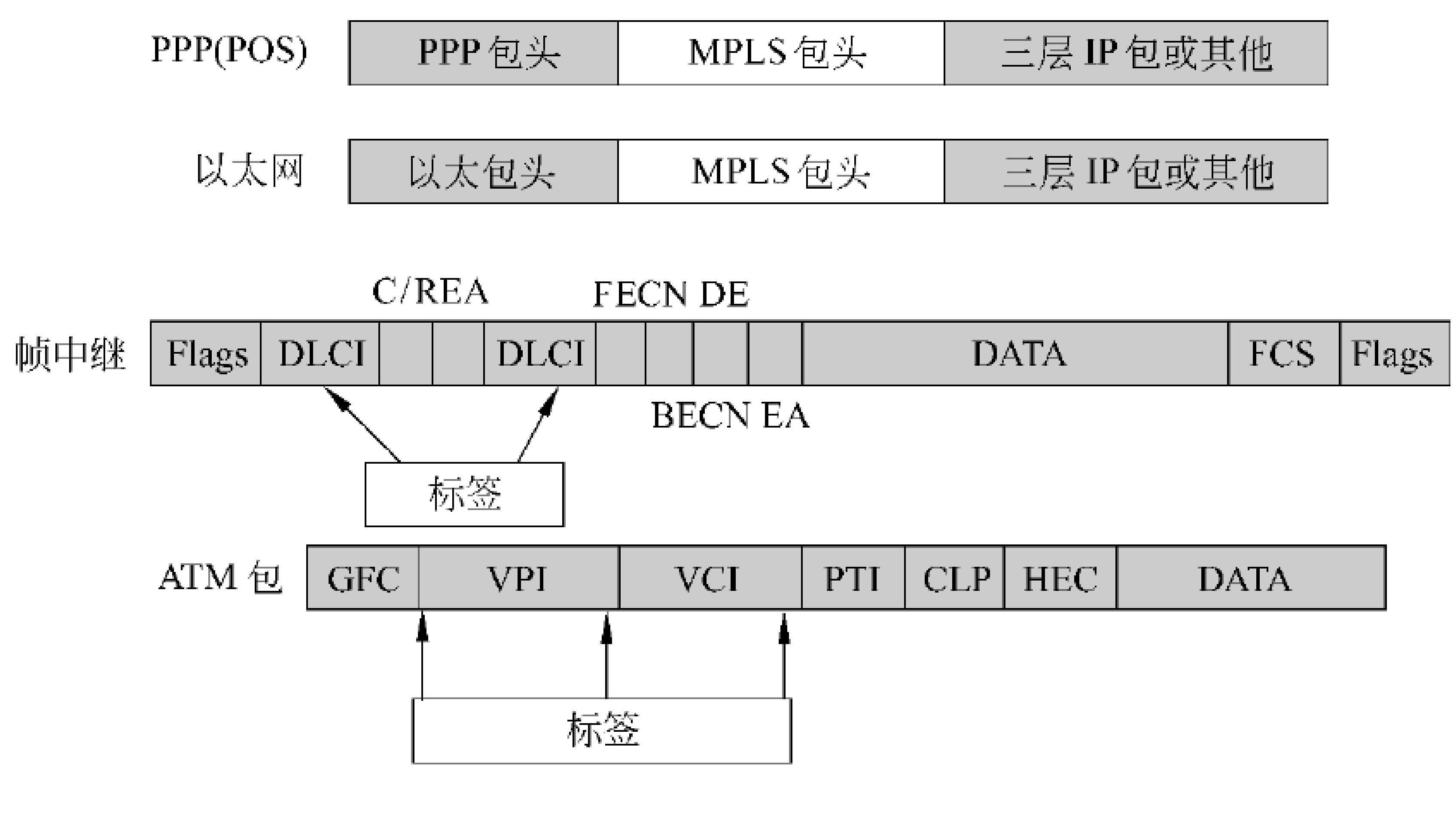


图 A-15　不同网络中 MPLS 包头结构

A.8　IPSec VPN 技术

关于 IPSec VPN 技术在生活中的应用，先看一个实际的例子。

某人通过网络购买一本《数字化生存》，当网络订单传递到书店时，问题出现了。管理员想知道这是一个真的订单吗？它真的是从客户那里发送出来的吗？订单在传输的过程中被黑客修改过？黑客会不会把订购数目从 1 本改成 100 本，或把地址做修改？这样的例子举不胜举，只要有信息在网上传递，就需要考虑信息源的可靠性和数据的完整性。

第三层隧道协议 IPSec 协议可以有效解决以上疑问，IPSec 协议是一个应用广泛、开放的 VPN 安全协议，它提供所有在网络层上的数据保护，进行透明的安全通信。

众所周知，当数据在公网上传输时，IP 包本身并不继承任何安全特性，所以很容易便可伪造出 IP 包的地址、修改其内容、重播以前的包以及在传输途中拦截并查看包的内容。因此不能确认是否收到正确的 IP 数据报。

(1) 来自原先要求的发送方；

(2) 包含的是发送方当初放在其中的原始数据；

(3) 原始数据在传输中途未被其他人看过。

针对以上这些问题，IPSec 可有效地保护 IP 数据报的安全。IPSec 主要功能是为 IP 通信中数据包提供加密和认证，为 IP 网络通信提供透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，可以有效抵御网络攻击，支持 IP 网络上数据的安全传输。它采取的具体保护形式包括：数据起源地验证；无连接数据的完整性验证；数据内容的机密性验证；抗重播保护；以及有限的数据流机密性保证。

IPSec 是 IETF 组织制定的第三层隧道协议，IPSec 为保障 IP 数据报的安全，定义了一个特殊的方法，它规定了要保护什么通信、如何保护它以及通信数据发给何人，以保证在 Internet 上传送数据的安全性。特定通信方之间在 IP 层，使用 IPSec 协议来加密数据源与验证数据源，确保数据包在 Internet 上传输时的私有性、完整性和真实性。

IPSec 不是一个单独协议，而是一组开放协议总称，是应用于 IP 层网络数据安全的一整套体系结构，它包括网络安全协议 AH 协议和 ESP 协议、密钥管理协议 IKE 协议和用于网络验证及加密的一些算法等。为保证数据安全，IPSec 使用 IKE 进行协议及算法协商，采用由 IKE 生成密码来加密和验证，在 IP 层提供安全服务，对 IP 及所承载的数据提供保护，这些保护通过两个安全协议 AH 和 ESP 加密实现。如图 A-16 给出了各协议之间的关系。

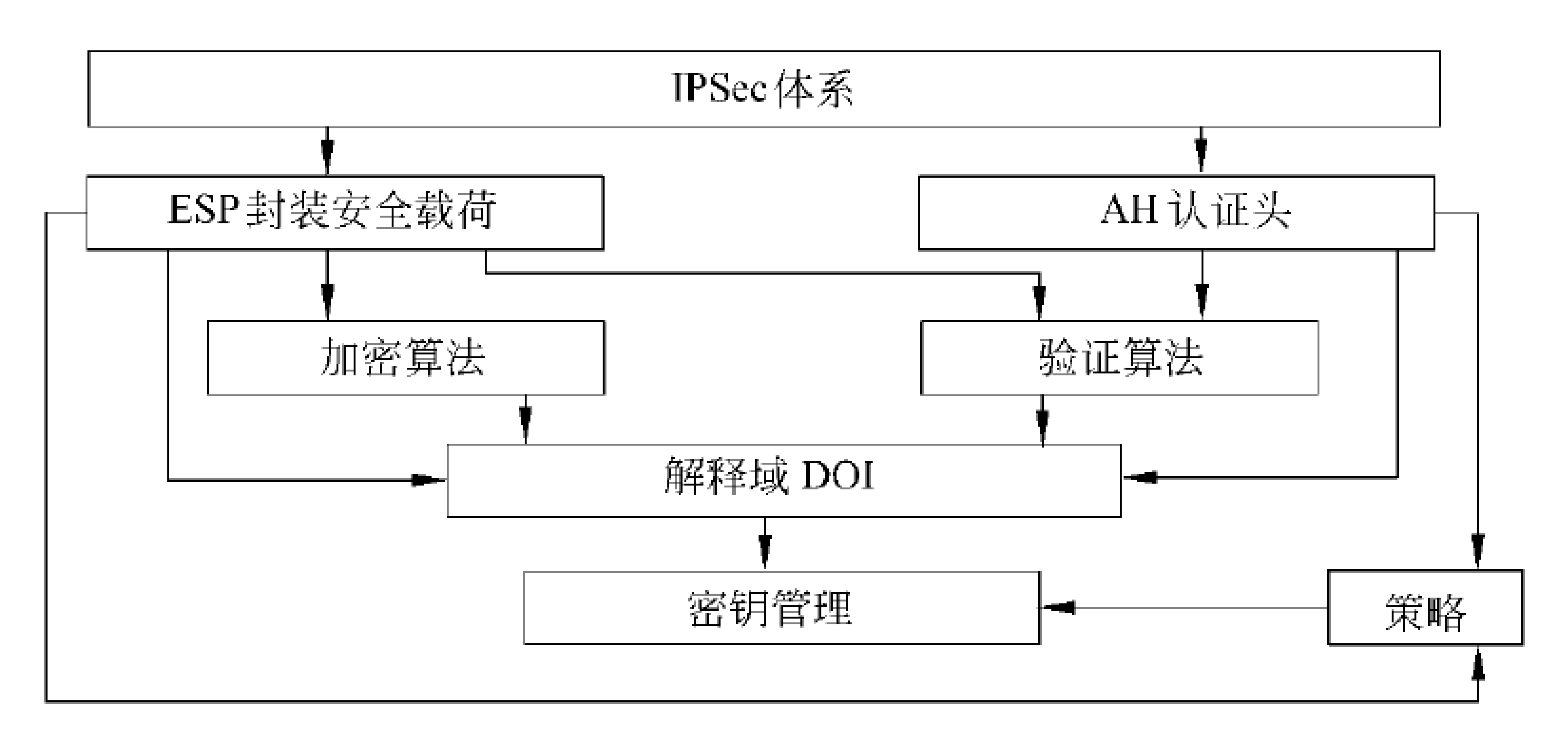


图 A-16　IPSec 协议体系结构

对 IPSec 协议体系结构详细说明如下：

① AH 为 IP 数据包提供无连接数据完整性和数据源身份认证，同时具有防重放攻击能力。数据完整性校验通过消息认证码（如 MD5）产生校验值来保证；数据源身份认证通过在待认证的数据中加入一个共享密钥来实现；AH 报头中序列号可以防止重放攻击。

② ESP 为 IP 数据包提供数据的保密性（通过加密机制）、无连接的数据完整性、数据源身份认证以及防重放攻击保护。与 AH 相比，数据保密性是 ESP 的新增功能，数据源身份认证、数据完整性检验以及重放保护都是 AH 可以实现的。

③ AH 和 ESP 可以单独使用，也可以配合使用。通过这些组合方式，可以在两台主机、两台安全网管（防火墙和路由器）或者主机与安全网管之间配置多种灵活的安全机制。

④ 解释域（DOI）将所有的 IPSec 协议捆绑在一起，是 IPSec 安全参数的主要数据库。

⑤ 密钥管理包括 IKE 协议和安全联盟（SA）等部分。IKE 在通信系统之间建立安全联盟，提供密钥管理和密钥确定的机制，是一个产生和交换密钥材料并协调 IPSec 参数的框架。

IPSec 协议族中的包括三个主要协议，各部分的功能如下。

1. AH 协议

IPSec 认证包头 AH 是一个用于提供 IP 数据报完整性和认证的机制，其完整性是保证数据包不被无意或恶意的方式改变，而认证则验证数据的来源（识别主机、用户、网络等）。在网上实现 IPSec 安全通信，将 AH 插到标准 IP 包头后面，AH 采用安全哈希算法来对数据包进行保护，保证数据包的完整性和真实性，防止黑客截断数据包或向网络中插入伪造的数据包，如图 A-17 所示。

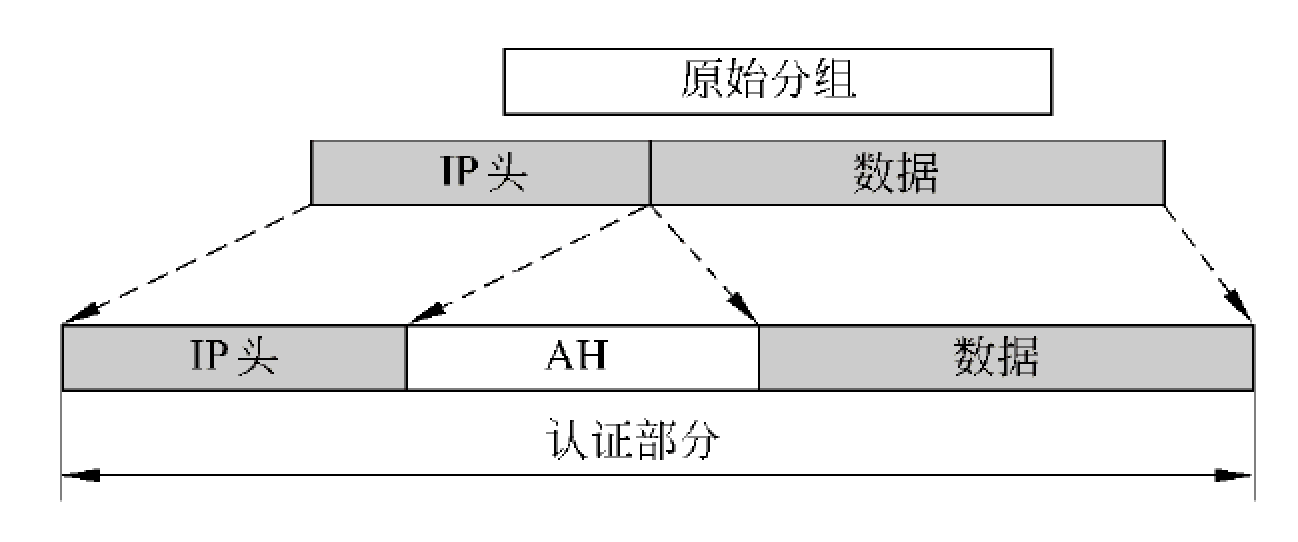


图 A-17 AH 对 IP 包头封装

AH 使用的包头放在标准的 IPv4 和 IPv6 包头和下一个高层协议帧(如 TCP、UDP、ICMP 等)之间,如图 A-18 所示。

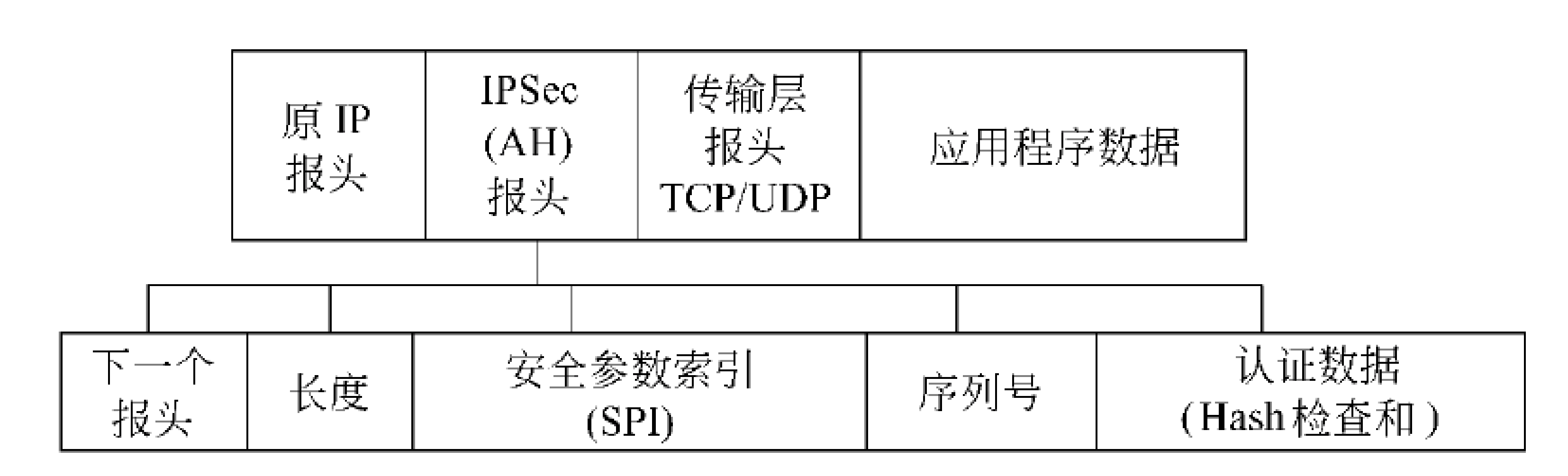


图 A-18 IPSec 协议包中 AH 协议

其中:

- 下一个报头(Next Header 8 位)——该字段包含跟在 IPSec 头之后的第四层协议头的协议号。如果第四层协议是 TCP,这个字段的值是 6。对于 UDP,它的值将是 17。
- 长度(Payload Length 8 位)——这个字段包含 IPSec 协议头长度减 2 的值。
- 安全参数索引(Security Parameters Index 32 位)——目的 IP 地址、IPSec 协议以及编号,它们用来唯一地为这个分组确定 SA。
- 序列号(Sequence Number Field 32 位)——这是一个无符号单调递增的计数器,对于一个特定的 SA,它实现反重传服务。这些信息不被接收对等实体使用,但是发送方必须包含这些信息。当建立一个 SA 时,这个值被初始化为 0。

AH 包头可以保证信息源的可靠性和数据的完整性。首先发送方 IP 包头、高层的数据、公共密钥这三部分通过某种散列算法进行计算,得出 AH 包头中的验证数据,并将 AH 包头加入数据包中;当数据传输到接收方时,接收方将收到 IP 包头、数据、公共密钥以相同的散列算法进行运算,并把得出的结果同收到数据包中的 AH 包头进行比较;如果结果相同则表明数据在传输过程中没有被修改,并且是从真正的信息源处发出。

AH 协议通过在整个 IP 数据报中实施一个消息文摘计算来提供完整性和认证服务。一个消息文摘就是一个特定的单向数据函数,它能够创建数据报的唯一的数字指纹。消息文摘算法的输出结果放到 AH 包头的认证数据(Authentication_Data)区。消息文摘算法 MD5 是一个单向数学函数。当应用到分组数据中时,它将整个数据分割成若干个 128b 的信息分组。每个 128b 为一组的信息是大分组数据的压缩或摘要的表示。当以这种方式使用时,MD5 只提供数字的完整性服务。一个消息文摘在被发送之前和数据被接

收到以后都可以根据一组数据计算出来。如果两次计算出来的文摘值是一样的，那么分组数据在传输过程中就没有被改变，这样就防止了无意或恶意的窜改。

在使用 HMAC-MD5 认证过的数据交换中，发送者使用以前交换过的密钥来首次计算数据报的 64b 分组的 MD5 文摘。从一系列的 16b 中计算出来的文摘值被累加成一个值，然后放到 AH 包头的认证数据区，随后数据报被发送给接收者。接收者也必须知道密钥值，以便计算出正确的消息文摘，并且将其与接收到的认证消息文摘进行适配。如果计算出的和接收到的文摘值相等，那么数据报在发送过程中就没有被改变，而且可以相信是由只知道秘密密钥的另一方发送的。

AH 不能提供加密服务，但为 IP 通信提供数据源认证和数据完整性检验，它能保护通信免受篡改，数据源认证以及可选的反重传服务，由于其并不加密传输内容，不能防止窃听，这就意味着分组将以明文形式传送。AH 提供数据完整性，保护其在发送接收端，使用共享密钥来保证身份真实性；使用 Hash 算法在每一个数据包上添加一个身份验证报头，来实现数据完整性检验。因此在通信过程中，需要预约好收发两端 Hash 算法和共享密钥。

2. ESP 协议

由于 AH 没有对用户数据进行加密。如果黑客使用协议分析仪照样可以窃取在网络中传输的敏感信息，所以使用有效负载安全封装(ESP) 协议把需要保护的用户数据进行加密，并放到 IP 包中，ESP 提供数据的完整性、可靠性。

ESP 主要区别于 AH 协议的是它的数据安全性保证，它使用预约好的加密算法和密钥对 IP 包进行加密，防止窃听。它也提供 AH 类似的数据源认证和数据完整性检验。AH 协议与 ESP 协议可以联合使用，也可以单独使用。

该协议通过原始分组的加密来提供数据机密性。另外，ESP 还提供数据源认证、完整性服务、反重传服务以及一些有限制的流量的机密性。当在 IPSec 流量中需要数据机密性时，应该使用 ESP 协议。ESP 协议的工作方式与 AH 不一样。正如它的名字暗示的那样，ESP 使用一个头和一个尾包围原始的数据报，从而封装它的全部或部分内容。如图 A-19 所示给出了 ESP 协议封装的过程。

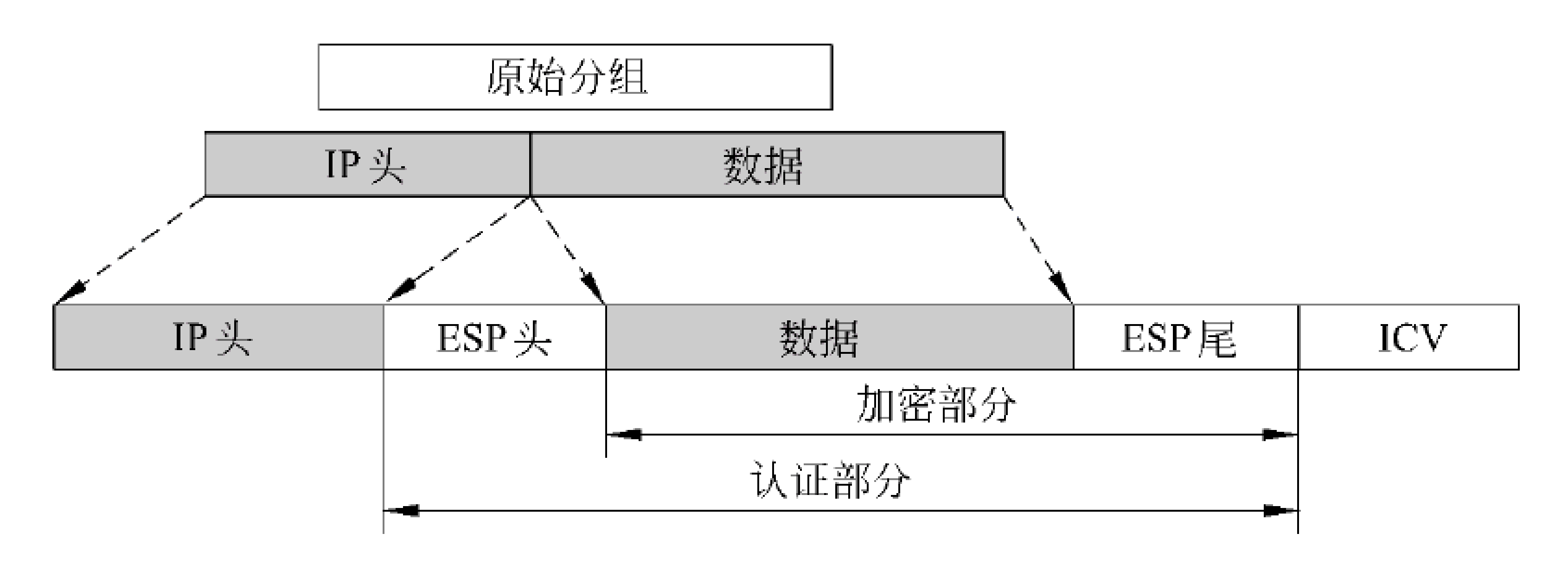


图 A-19　ESP 协议封装的过程

3. Internet 密钥交换协议 IKE

无论实现 AH 或 ESP 还是两者的联合，收发端两台计算机必须首先建立某种约定，

这种约定称为“安全关联”。安全关联指双方需要就如何保护信息、交换信息等公用的安全设置达成一致。Internet 密钥交换协议(IKE)用于在两个通信实体协商和建立安全相关,交换密钥。安全相关(Security Association)是 IPSec 中的一个重要概念,一个安全关联表示两个或多个通信实体之间经过了身份认证,且这些通信实体都能支持相同的加密算法,成功地交换了会话密钥,可以开始利用 IPSec 进行安全通信。IPSec 协议本身没有提供在通信实体间建立安全关联的方法,利用 IKE 建立安全关联。IKE 定义了通信实体间进行身份认证、协商加密算法以及生成共享的会话密钥的方法,如图 A-20 所示。IKE 中身份认证采用共享密钥和数字签名两种方式,密钥交换采用 Diffie-Hellman 协议。

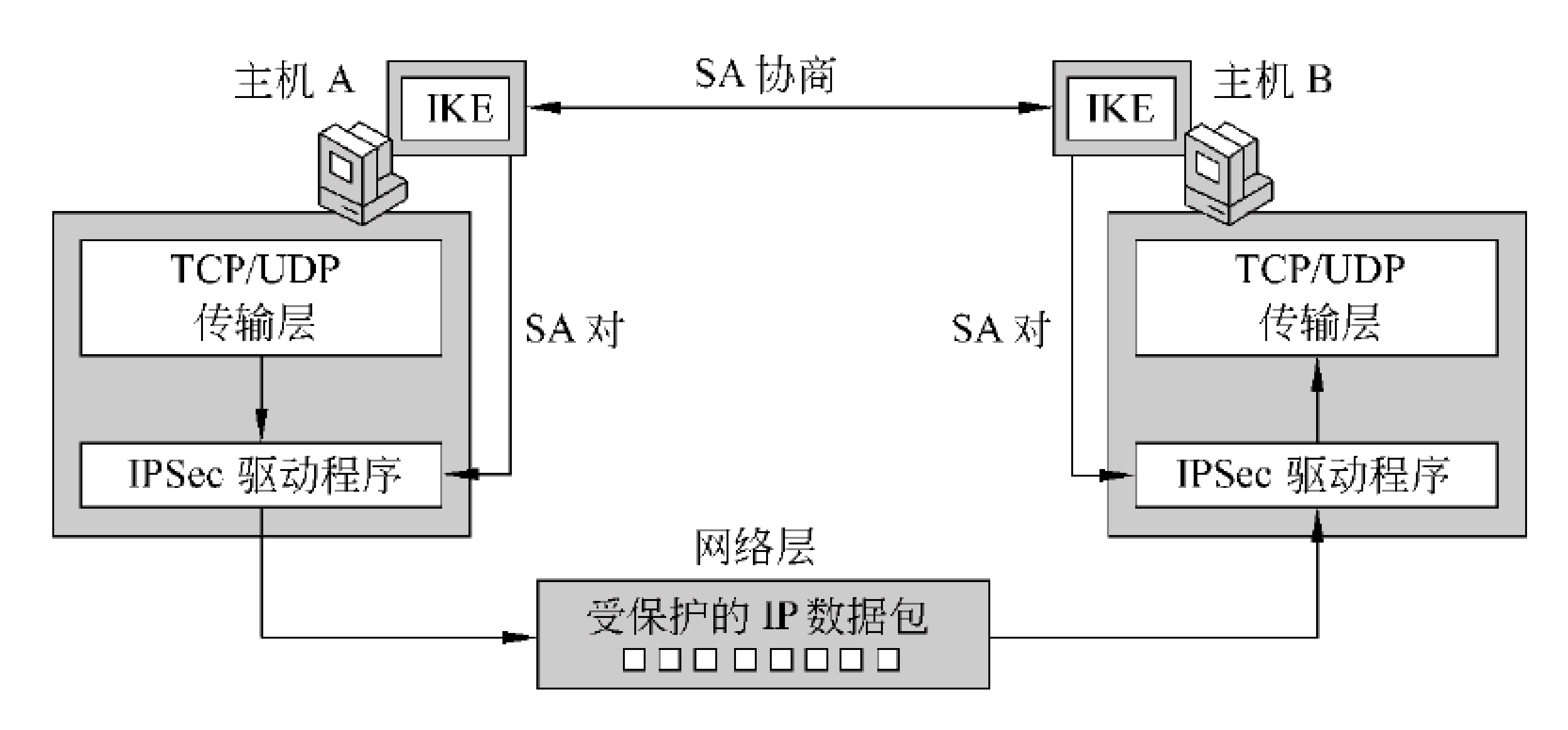


图 A-20 IKE 在两个通信实体协商和建立安全相关

IKE 协议主要是对密钥交换进行管理,主要包括对使用的协议、加密算法和密钥进行协商,建立可靠的密钥交换机制。IKE 是一个混合协议,它使用到了三个不同协议的相关部分:安全关联和密钥交换协议 ISAKMP,密钥确定协议 OAKLEY 和 SKEME。

IPSec 通过 AH 和 ESP 这两个安全协议来实现对 IP 数据报或上层协议的保护,而且此实现不会对用户主机或其他 Internet 组件造成影响,用户还可以选择不同的加密算法而不会影响其他部分的实现。

AH 是报文验证头协议,主要提供的功能有数据源验证、数据完整性校验和防报文重放功能。ESP 是封装安全载荷协议,它除提供 AH 协议的所有功能之外,还可提供对 IP 报文的加密功能。AH 和 ESP 可以单独使用,也可以同时使用。

IPSec 协议可以设置成在两种模式下运行:一种是隧道(Tunnel)模式,一种是传输(Transport)模式。传输模式只对 IP 数据包的有效负载进行加密或认证,此时继续使用原始 IP 头部。传输模式对 IP 包的路由支持较好。隧道模式对整个 IP 数据包进行加密或认证。此时,需要新产生一个 IP 头部,原来 IP 头被加密,有效地防止“中间人”攻击。传输模式是为了保护端到端的安全性,即在这种模式下不会隐藏路由信息,如图 A-21 所示。

在隧道模式下,IPSec 把 IPv4 数据包封装在安全的 IP 帧中,这样保护从一个防火墙到另一个防火墙时的安全性。在隧道模式下,信息封装是为了保护端到端的安全性,即在这种模式下不会隐藏路由信息。隧道模式是最安全的,但会带来较大的系统开销。

如图 A-22 所示 IPSec 的安全体系可以看出,IPSec 提供的安全服务还需要用到共享密钥,因特网密钥交换协议,为 IPSec 提供了自动协商交换密钥,建立和维护安全联盟的

服务，能够简化 IPSec 使用和管理。

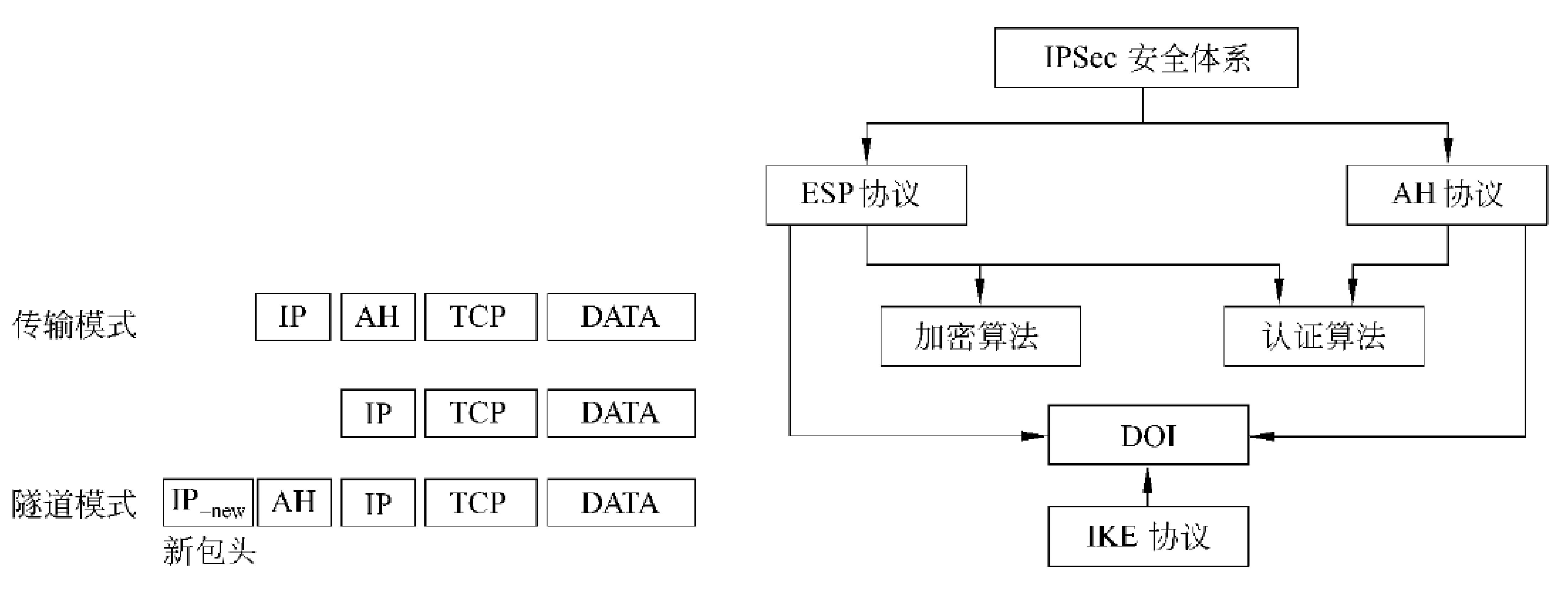


图 A-21　IPSec 协议工作模式　　　　图 A-22　IPSec 协议的组成体系

安全策略按照优先级的先后顺序，创建可供使用的加密和隧道机制以及验证方式。当需要建立通信时，双方机器执行相互验证，然后协商使用何种加密方式。此后的所有数据流都将使用双方协商的加密机制进行加密，然后封装在隧道包头内。

IPSec 协议的优点：它定义了一套用于保护私有性和完整性的标准协议；IPSec 支持一系列加密算法如 DES、3DES、IDEA；它检查传输的数据包的完整性，以确保数据没有被修改，具有数据源认证功能；IPSec 可确保运行在 TCP/IP 协议上的 VPN 之间的互操作性。

IPSec 隧道模式具有以下局限：IPSec 需要已知范围 IP 地址或固定范围 IP 地址，因此在动态分配地址时不太适合于 IPSec；除了 TCP/IP 协议以外，IPSec 不支持其他协议，只能支持 IP 数据流；除了包过滤外，它没有指定其他访问控制方法；对于采用 NAT 方式访问公共网络的情况难以处理；IPSec 目前还仅支持单播的（Unicast）IP 数据包，不支持多播（Multicast）和广播（Broadcast）的 IP 数据包。

A.9　SSL VPN 技术

关于 SSL VPN 技术在生活中的应用，先看一个实际的例子。

XXXX 公司的分公司、办事处和移动办公员工需要访问财务、人力资源和工程信息管理系统以及其他数据库、文件等应用服务器。这些应用系统的用户分布在网络的各个位置，接入方式各式各样，如 ADSL 宽带、拨号、无线等。需要在保证应用系统稳定可靠运行的前提下，重视应用数据在服务器与用户终端之间传输的安全性也非常重要，所以数据的私密性、完整性对于整个集团的核心业务信息是重点考虑问题。

针对公司的这种网络应用状况，在规划网络时，需要考虑如下要素。

(1) 能够提供安全的通道，解决办事处人员远程访问，保证分公司和总公司连通性；

(2) 保证基于 Web 的业务系统正常、稳定运行；

(3) 尽最大可能保证用户当前的网络拓扑不被修改；

SSL VPN 技术可以很好解决以上遇到的网络安全问题。

第三层隧道协议 SSL(Secure Socket Layer)最初由网景公司开发,现已成为鉴别网站和网页浏览者身份,以及客户机及服务器之间进行加密通信的全球化标准。由于 SSL 技术已内嵌到所有的主流浏览器和 Web 服务器程序中,因此仅需安装数字证书,或服务器证书,就可以激活服务器安全服务功能。

SSL VPN 利用用户浏览器内建的 Secure Socket Layer 封包处理功能,用浏览器连回公司内部 SSL VPN 服务器,然后通过网络封包的方式,让使用者的客户机可以在远程计算机执行应用程序,读取公司内部服务器数据。这一传输过程采用标准的 SSL 对传输中的数据包进行加密,从而在应用层保护了数据的安全性。高质量的 SSL VPN 解决方案可保证企业进行安全的全局访问。

在不断扩展的互联网 Web 站点之间、远程办公室、传统交易大厅和移动客户端间,SSL VPN 克服了 IPSec VPN 的不足,用户可以轻松实现安全易用、无需客户端安装,且配置简单的远程访问,从而降低用户的总成本并增加远程用户的工作效率。而在这些同样网络环境中,由于网络地址转换(NAT)和防火墙配置技术,IPSec VPN 在这样的网络结构中则难以实现,因为 IPSec VPN 很难实现防火墙和 NAT 遍历,无力解决 IP 地址冲突。相对于传统 IPSec VPN 而言,SSL VPN 似乎正好可以跟它互补。

SSL 协议是一种在 Internet 上保证发送信息安全的通用协议,SSL 用公钥加密,通过 SSL 连接来完成传输的数据来工作,指定应用程序协议(如 HTTP、Telnet 和 FTP 等)和底层协议之间,进行数据的安全交换机制,为在 TCP/IP 通信的网络连接中,提供数据加密、服务器认证以及可选的客户机认证服务。

SSL 安全协议主要提供以下方面的安全认证服务。

(1) 客户机和服务器的合法性认证。

确认客户机和服务器合法性,提供安全认证服务,使数据能够确信被发送到正确的客户机和服务器上。客户机和服务器都有各自识别号,这些识别号由公开密钥进行编号,为了验证用户是否合法,安全套接层协议要求在握手交换数据时进行数字认证,以此来确保用户合法性。

(2) 加密、隐藏被传送的数据。

安全套接层协议所采用的加密技术既有对称密钥技术,也有公开密钥技术。在客户机与服务器进行数据交换之前,交换 SSL 初始握手信息,在 SSL 握手信息中,采用各种加密技术对其加密,以保证其机密性和数据的完整性,并且用数字证书进行鉴别,这样就可以防止非法用户进行破译,如图 A-23 所示。

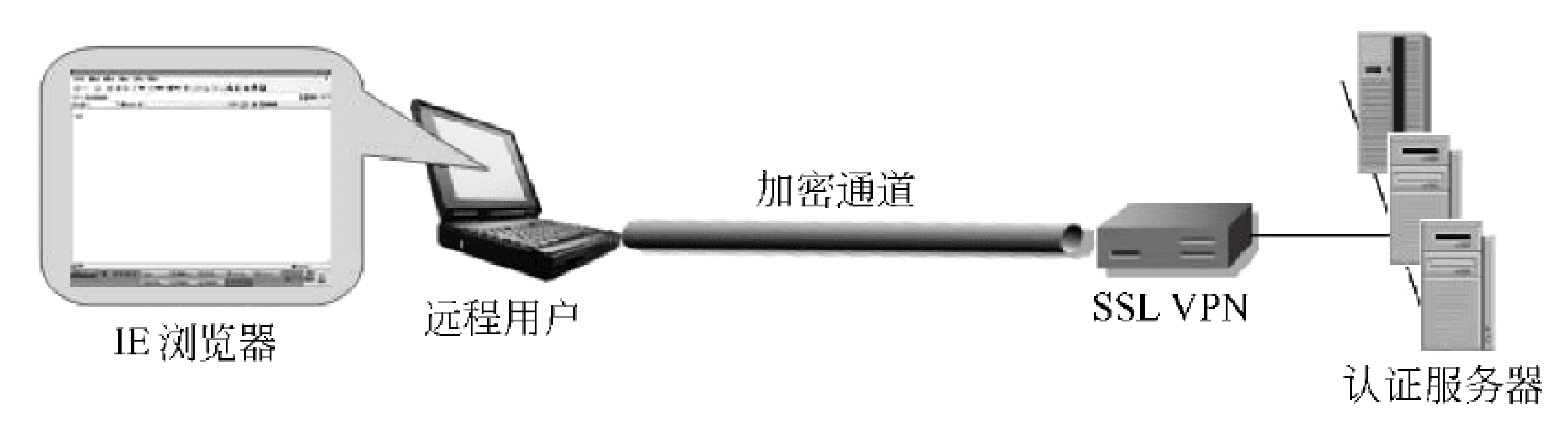


图 A-23 密钥技术加密数据以隐藏传送

除了无客户端、有很高的安全性以外，最重要的是，它可以充分发掘企业应用的潜能。很多企业已经建成了 OA 系统、ERP 系统，接下来，就希望能够充分利用这些系统。通过 SSL VPN，无论是员工、合作伙伴还是客户，都能够访问所需的应用。利用 Internet 让企业现有应用发挥更大的作用，这才是 SSL VPN 的价值所在。

SSL VPN 则最适合下述情况：企业需要通过互联网(笔记本型计算机、家用个人计算机、Internet 信息站点接入)，达到广泛而全面的信息存取，即 SSL VPN 更加适合用来解决点到网的互联问题。如果一个企业同时存在网间互连和点到网的互联需求，必须根据远程访问的需求与目标而定，在需要点到网互联的时候，使用 SSL 技术最合适满足用户的需求；在需要网到网互连的时候，使用 IPSec 最合适。当企业需要安全的点对点连接，或用单一装置进行远程访问，并且让企业拥有管理所有远程访问使用者能力时，IPSec 可能是最适合的解决方案，即 IPSec 更加适合用来解决网到网的互联问题。

SSL 协议的主要用途是在两个通信应用程序之间提供私密性和可靠性，SSL 协议由许多子协议组成，其子协议包括握手协议、记录协议以及警告协议三部分。握手协议负责确定用于客户机和服务器之间的会话加密参数；记录协议用于交换应用数据；警告协议用于在发生错误时终止两个主机之间的会话；各部分完成的功能如下。

(1) 握手协议：负责客户机和服务器之间会话的加密参数。当一个 SSL 客户机和服务器第一次开始通信时，传输第一数据字节以前，彼此确认，协商一种加密算法和密码钥匙，在一个协议版本上达成一致，选择认证方式，并使用公钥技术来生成共享密钥。在数据传输期间，记录协议利用握手协议生成的密钥，加密和解密后来交换的数据。

(2) 记录协议：用于交换应用数据。应用程序消息被分割成可管理的多个数据块，还可以压缩，并产生一个 MAC(消息认证代码)，然后被加密并传输。接收方接收数据并对它解密，校验 MAC，解压并重新组合，把结果提供给应用程序协议。

(3) 警告协议：用于提示在什么时候发生了错误，或两个主机之间的会话在什么时候终止。

两个主要的子协议是握手协议和记录协议，提供了数据私密性、端点验证、信息完整性等特性。SSL 协议通信的握手步骤如下。

第一步，SSL 客户机连接至 SSL 服务器，并要求服务器验证它自身的身份。

第二步，服务器通过发送它的数字证书证明其身份。这个交换还可以包括整个证书链，直到某个根证书颁发企业(CA)。通过检查有效日期并确认证书包含可信任 CA 的数字签名来验证证书的有效性。

第三步，服务器发出一个请求，对客户端的证书进行验证，但是由于缺乏公钥体系结构，当今的大多数服务器不进行客户端认证。

第四步，协商用于加密的消息加密算法和用于完整性检查的哈希函数，通常由客户端提供它支持的所有算法列表，然后由服务器选择最强大的加密算法。

第五步，客户机和服务器通过以下步骤生成会话密钥。

客户机生成一个随机数，并使用服务器的公钥(从服务器证书中获取)对它加密，以送到服务器上。服务器用更加随机的数据(客户机的密钥可用时则使用客户机密钥，否则以明文方式发送数据)响应。使用哈希函数从随机数据中生成密钥。

SSL VPN 一般的实现方式是在浏览器中设置 SSL 代理服务器。首先浏览与代理服务器建立 TCP 连接,并向其发出与远端 Web 服务器连接的消息,然后代理服务器与 Web 服务器建立 TCP 连接,此时这个代理服务器完全成为内容转发装置。浏览器与 Web 服务器建立了一个安全通道,由于这个安全通道是端到端的,尽管所有的消息经过代理服务器,但其内容代理服务器是无法解密和改动的。

一个完整 SSL VPN 的运行步骤如下。

管理员在配置完 SSL VPN 资源之后,远程终端用户首先通过 SSL 协议来访问总部 SSL VPN。用户在浏览器的地址栏输入 HTTPS 格式的访问地址,在 HTTP 层将用户需求翻译成 HTTP 请求并送至 SSL 层;SSL 层借助下层协议的信道协商出一份加密密钥,并用此密钥来加密 HTTP 请求;加密后的 HTTP 请求通过 TCP 层的 443 端口与 SSL VPN 建立连接,传递 SSL 处理后的数据。

SSL VPN 收到加密的数据包之后,在 SSL 层通过协商出的加密密钥来解密,再将翻译出的数据送至应用层。此后,远程终端用户将打开 SSL VPN 的资源管理 Web 页面,并在 HTTP 层下载 Active 控件来协商与中心 SSL VPN 的隧道,终端用户通过与总部 SSL VPN 已经建立的加密连接,协商隧道的加密算法、验证算法以及进行端口转换的端口号和通信协议。隧道协商成功之后,客户端将会启动一个虚拟网卡,并显示为已连接的状态,此后可信任资源的访问都将通过 SSL VPN 加密传输。

远程终端用户通过 SSL VPN 访问应用数据的时候,传输过程如下。

① 应用程序把应用数据提交至本地的 SSL;

② 远程终端用户根据需要指定的压缩算法,压缩应用数据;

③ 远程终端用户把应用数据用加密算法加密,再按照指定的协议和端口号通过公网网络传输到总部 SSL VPN 网关;

④ SSL VPN 网关用相同的加密算法对密文进行解密,得到明文;

⑤ SSL VPN 网关用相同的散列算法对明文中的应用数据散列,计算得到的散列值和明文的散列值比较,如果一致,则明文有效;否则丢弃该报文。

⑥ SSL VPN 网关将明文应用数据转发到保护子网的资源主机,资源主机对该应用数据包处理之后再向远程终端用户回包;

⑦ 经过 SSL VPN 网关的加密后(同远程终端相同步骤),再传输至远程终端用户;

⑧ 远程终端用户的 SSL 层接收加密包后再使用解密算法解密,并将该应用数据包发送至用户的应用层。

至此,一个数据包经过 SSL VPN 传输的过程完毕,如图 A-24 所示。

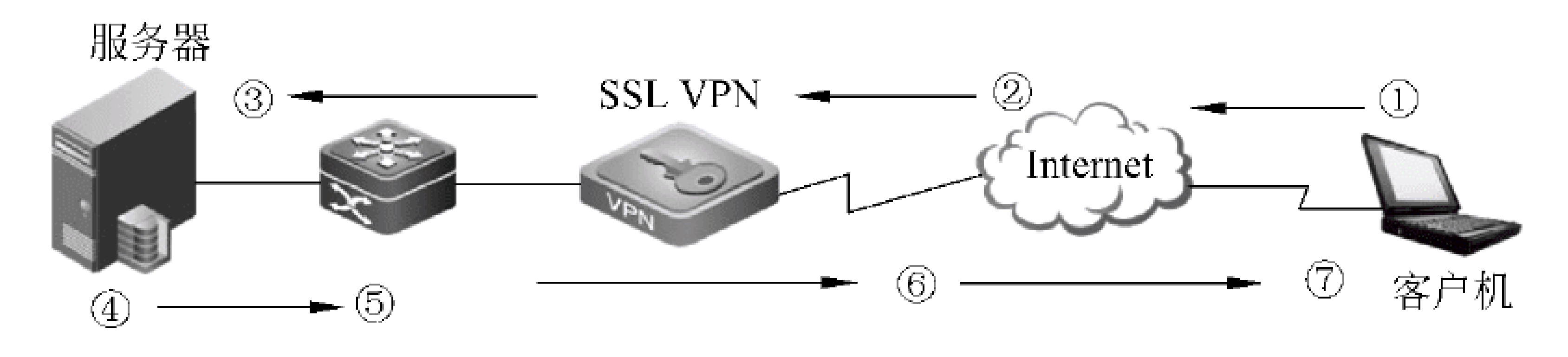


图 A-24　SSL VPN 传输流程

① 本地应用数据的加密；

② 加密数据传送至 SSL VPN 网关；

③ SSL VPN 网关将解密的数据传送至应用服务器；

④ 应用服务器的处理；

⑤ 处理后的数据传送至 SSL VPN 网关；

⑥ SSL VPN 网关加密数据包后传送至远端用户；

⑦ 本地接收到数据后解密以及应用；

SSL VPN 是解决远程用户访问敏感公司数据最简单最安全的解决技术，与复杂的 IPSec VPN 相比，SSL VPN 通过简单易用的方法实现信息远程连通。任何安装浏览器的机器都可以使用 SSL VPN，这是因为 SSL 内嵌在浏览器中，不需要像传统 IPSec VPN 一样必须为每一台客户机安装客户端软件。

SSL 独立于应用，任何一个应用程序都可以享受它的安全性而不必理会执行细节。此外 SSL 本身就被几乎所有的 Web 浏览器支持，这意味着客户端不需要为了支持 SSL 连接安装额外的软件。SSL VPN 的目标是确保用户随时随地安全存取企业信息，是一种低成本、高安全性、简便易用的远程访问 VPN 解决方案，非常适合以 Web 应用为主、有大量客户端的用户。

SSL VPN 的主要优点表现在下面几个主要的方面。

(1) 无需安装客户端软件：在大多数执行基于 SSL 协议的远程访问是不需要在远程客户端设备上安装软件。只需通过标准的 Web 浏览器连接因特网，即可以通过网页访问到企业总部的网络资源。这样无论是从软件协议购买成本上，还是从维护、管理成本上都可以节省一大笔资金，特别是对于大、中型企业和网络服务提供商。

(2) 适用大多数设备：基于 Web 访问的开放体系可以在运行标准的浏览器下可以访问任何设备，包括非传统设备，如可以上网的电话和 PDA 通信产品。这些产品目前正在逐渐普及，因为它们在不进行远程访问时也是一种非常理想的现代时尚产品。

(3) 适用于大多数操作系统：可以运行标准的因特网浏览器的大多数操作系统都可以用来进行基于 Web 的远程访问，不管操作系统是 Windows、Macintosh、UNIX 还是 Linux。可以对企业内部网站和 Web 站点进行全面的访问。用户可以非常容易地得到基于企业内部网站的资源，并进行应用。

(4) 支持网络驱动器访问：用户通过 SSL VPN 通信可以访问在网络驱动器上的资源。

(5) 良好的安全性：用户通过基于 SSL 的 Web 访问并不是网络的真实节点，就像 IPSec 安全协议一样，而且还可代理访问公司内部资源。因此，这种方法可以非常安全的，特别是对于外部用户的访问。

(6) 较强的资源控制能力：基于 Web 的代理访问允许公司为远程访问用户进行详尽的资源访问控制。

(7) 减少费用：为那些简单远程访问用户(仅需进入公司内部网站或者进行 Email 通信)，基于 SSL 的 VPN 网络可以非常经济地提供远程访问服务。

(8) 可以绕过防火墙和代理服务器进行访问：基于 SSL 的远程访问方案中，使用

NAT(网络地址转换)服务的远程用户或者因特网代理服务的用户可以从中受益,因为这种方案可以绕过防火墙和代理服务器进行访问公司资源,这是采用基于 IPSec 安全协议的远程访问所很难或者根本做不到的。

上面介绍 SSL VPN 技术这么多优势,那么为什么现在不是所有用户都使用 SSL VPN,且据权威调查企业调查显示目前绝大多部分企业仍采用 IPSec VPN 呢? SSL VPN 的主要不足在哪里呢?

(1) 必须依靠因特网进行访问:为了通过基于 SSL VPN 进行远程工作,当前必须与因特网保持连通性。因为此时 Web 浏览器实质上是扮演客户服务器的角色,远程用户的 Web 浏览器依靠公司的服务器进行所有进程。正因如此,如果因特网没有连通,远程用户就不能与总部网络进行连接,只能单独工作。

(2) 对新的或者复杂的 Web 技术提供有限支持:基于 SSL 的 VPN 方案是依赖于反代理技术来访问公司网络的。因为远程用户是从公用因特网来访问公司网络的,而公司内部网络信息通常不仅是处于防火墙后面,而且通常是处于没有内部网 IP 地址路由表的空间中。反代理的工作就是翻译出远程用户 Web 浏览器的需求,通常使用常见的 URL 地址重写方法,例如,内部网站也许使用内部 DNS 服务器地址链接到其他的内部网链接,而 URL 地址重写必需完全正确地读出以上链接信息,并且重写这些 URL 地址,以便这些链接可以通过反代理技术获得路由,当有需要时,远程用户可以轻松地通过单击路由进入公司内部网络。对于 URL 地址重写器完全正确理解所传输的网页结构是极其重要的,只有这样才可正确显示重写后的网页,并在远程用户计算机浏览器上进行正确地操作。

(3) 只能有限地支持 Windows 应用或者其他非 Web 系统:因为大多数基于 SSL 的 VPN 都是基 Web 浏览器工作的,远程用户不能在 Windows、UNIX、Linux、AS400 或者大型系统上进行非基于 Web 界面的应用。虽然有些 SSL 提供商已经开始合并终端服务来提供上述非 Web 应用,但不管如何,目前 SSL VPN 还未正式提出全面支持,这一技术还有待讨论,也可算是一个挑战。

(4) 只能为访问资源提供有限安全保障:当使用基于 SSL 协议通过 Web 浏览器进行 VPN 通信时,对用户来说外部环境并不是完全安全、可达到无缝连接的。因为 SSL VPN 只对通信双方的某个应用通道进行加密,而不是对在通信双方的主机之间的整个通道进行加密。在通信时,在 Web 页面中呈现的文件很难也基本上无法保证只出现类似于上传的文件和邮件附件等简单的文件,这样就很难保证其他文件不被暴露在外部,存在一定的安全隐患。

参 考 文 献

[1] Merike Kaeo.网络安全性设计．北京：人民邮电出版社，2005.
[2] Andrew G Mason．Cisco安全虚拟专用网络．北京：人民邮电出版社，2003.
[3] 何宝宏，田辉．IP虚拟专用网技术．北京：人民邮电出版社，2008.
[4] 王达．虚拟专用网精解．北京：清华大学出版社，2004.
[5] David Leon Clark．虚拟专用网．北京：人民邮电出版社，2000.

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602　　计算机与信息分社营销室 收
邮编：100084　　电子邮件：jsjjc@tup.tsinghua.edu.cn
电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：VPN 虚拟专用网安全实践教程

ISBN：978-7-302-21234-8

个人资料

姓名：________________ 年龄：_______ 所在院校/专业：_____________________

文化程度：____________ 通信地址：_______________________________________

联系电话：____________ 电子信箱：_______________________________________

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议_______________________________

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议_______________________________

您对本书的总体满意度：

从语言质量角度看 □很满意 □满意 □一般 □不满意

从科技含量角度看 □很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？（可附页）

____

____

您希望本书在哪些方面进行改进？（可附页）

____

____